| NODIS Library | Organization and Administration(1000s) | Search |

NASA
Procedural
Requirements

NPR 1600.4A
Effective Date: April 08, 2016
Expiration Date: April 08, 2021

COMPLIANCE IS MANDATORY FOR NASA EMPLOYEES

Identity and Credential Management

Responsible Office: Office of Protective Services

NAII 1600.4A, Foreign National Access Management (FNAM) Operations Manual

Table of Contents

Preface

Chapter 1. Introduction

Chapter 2. Roles and Responsibilities

Chapter 3. Enrollment and Credential Issuance

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

Chapter 4. Foreign Nationals

Chapter 5. Characteristics of NASA Badges

Chapter 6. PIV Credential Management Lifecycle

Appendix A: Definitions
Appendix B: Acronyms

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

Preface

P.1 Purpose

a. This National Aeronautics and Space Administration (NASA) directive establishes Agency-wide identity, credential, and access management policy and establishes high-level implementation requirements as set forth in NASA Policy Directive (NPD) 1600.2, NASA Security Policy, as amended. Identity, credential, and access management are the activities that deal with identifying individuals and controlling their access to resources (e.g., facilities and information technology (IT) systems) by associating user rights and restrictions with the established identity.

b. This NASA directive prescribes personnel responsibilities and procedural requirements for the creation, usage, and management of identities and the creation and issuance of identity credentials to assist NASA Centers and Component Facilities in executing the NASA security program to protect people, property, and information.

P.2 Applicability

a. This NASA directive is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to Jet Propulsion Laboratory (JPL), a Federally Funded Research and Development Center (FFRDC), employees, JPL personnel, other contractors, grant recipients (to include recipients of cooperative agreements), or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

b. This NASA directive is applicable to all other personnel completing work through Space Act Agreements, Memorandums of Agreement/Understanding, or other applicable agreements, those assigned or detailed under the Intergovernmental Personnel Act, partners, and visitors.

c. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall" or "must." The terms: "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

d. In this directive, "NASA directives" refers to both Agency-level and Center-level directives.

e. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

f. This directive is applicable to NASA directives developed or revised after the effective date of this NPR.

P.3 Authority

National and Commercial Space Programs, 51 United States Code (U.S.C.) § 20132, Public Law (Pub. L.) 111-314, 124 Stat. 3328 (2010).

P.4 Applicable Documents and Forms

a. E-Government Act of 2002, 44 U.S.C. § 101.

b. Privacy Act of 1974, 5 U.S.C. § 552a.

c. Rehabilitation Act of 1973, 29 U.S.C. § 701.

d. Paperwork Reduction Act of 1980, 44 U.S.C. §§ 3501-3521.

e. Fraud and Related Activity in Connection with Computers, 18 U.S.C. § 1030.

f. Numbering System for Federal Accounts Relating to Individual Persons, Executive Order (E.O.) 9397, (1943).

g. Exchange Visitor Program, 22 CFR 62.

h. Office of Management and Budget (OMB) Memo M-05-24, August 5, 2005, "Implementation of Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standards for Federal Employees and Contractors."

i. NASA Procedural Directive (NPD) 1050.1, Authority to Enter Into Space Act Agreements.

j. NPD 1382.17, NASA Privacy Policy.

k. NPD 1440.6, NASA Records Management.

l. NASA Procedural Requirement (NPR) 1382.1, NASA Privacy Procedural Requirements.

m. NPR 1441.1, NASA Records Retention Schedules.

n. NPR 1600.1, Security Program Procedural Requirement.

o. NPR 1600.3, NASA Personnel Security.

p. NPR 1660.1, NASA Counterintelligence and Counterterrorism.

q. NPR 2190.1, NASA Export Control Program.

r. NPR 2200.2, Requirements for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information.

s. NPR 2810.1, Security of Information Technology.

t. NPR 2841.1, Identity, Credential, and Access Management Services.

u. NASA Identity Management and Account Exchange (IdMAX) System.

v. Department of Homeland Security, United States Customs and Border Protection, Form I-94, Arrival/Departure Record.

w. Homeland Security Presidential Directive 12 (HSPD-12), April 27, 2004.

x. Federal Information Processing Standards Publication (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

y. Federal Identity Credential and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011.

z. NIST SP 800-79-2, Guidelines for the Certification and Accreditation of Personal Identity Verification Card Issuers.

aa. NIST SP 800-104, A Scheme for PIV Visual Card Topography.

bb. Office of Personnel Management Electronic Questionnaire for Investigation Processing (e-QIP) System.

cc. Office of Personnel Management (OPM) Federal Investigations Notice No. 10-05, May 17, 2010, "Reminder to Agencies of the Standards for Issuing Credentials under HSPD-12."

P.5 Measurement/Verification

To determine compliance with this NASA directive, the Office of Protective Services (OPS) shall provide assessments/audits of the application of this policy requirement. This will consist of periodic reporting from the Centers, including information collected for the satisfaction of OMB. The specific metrics utilized will conform to those described in the latest version of the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance.

P.6 Cancellation

a. NPR 1600.4, Identity and Credential Management, dated August 12, 2012.

b. Memorandum for Center Directors, dated April 2, 2014, "Interim Policy Regarding Foreign National Access Management."

Chapter 1. Introduction

1.1 Overview

1.1.1 In recent years, the Federal Government has increased emphasis on improving the physical and logical security of the hundreds of thousands of facilities that it owns and leases, as well as the Information Technology (IT) systems to support the diverse mission work of Federal agencies. The Government Accountability Office (GAO) has identified the need to develop a common framework that includes key practices for guiding agencies' physical security efforts, such as employing a risk management approach to facility protection, leveraging advanced technology (e.g., smart cards), improving information sharing and coordination, and implementing performance measurement and testing. (See http://www.gao.gov/new.items/d0549.pdf). GAO has also outlined the need for standard performance metrics to evaluate the effectiveness of physical security protections.

1.1.2 This NASA directive establishes the policies and high-level procedures that shall be used throughout NASA to achieve the improvements in physical security protections required by GAO. Strong Identity, Credential, and Access Management (ICAM) practices and adherence to the Federal common framework for ICAM as outlined in the Federal ICAM (FICAM) Roadmap Guidance Document will address any weaknesses within NASA's physical security infrastructure.

1.1.3 Identity management and credential management allows the identity of an individual to be verified in the digital realm, so that identity can be trusted to conduct business. Even low-risk employees possess access behind physical and logical safeguards that can give them unprecedented access to critical information and systems. This document seeks to establish a common, standardized basis for ICAM within NASA.

1.1.4 ICAM business processes include all the processes necessary to support proofing and vetting the identity of all people requiring access (physical, logical, or both) to NASA resources. ICAM business processes also include all the necessary processes for issuing credential and granting access based on favorable identity proofing and vetting. The governance structure that has been established for ICAM business processes is documented in NPR 2841.1, Identity, Credential, and Access Management Services.

1.2 Scope

1.2.1 The policies and procedures identified within this document define the approved processes for NASA to manage personal identities and the issuance of NASA Personal Identity Verification (PIV) credentials. This NPR also establishes the policy for the management of other types of NASA non-PIV credentials, visitor badges, and alternate Agency credentials. Non-PIV logical access tokens are not covered in this document. Use of vetted and bound identity for physical access is covered by NPR 1600.1, and logical access is covered by NPR 2810.1 Security of Information Technology. The policies and procedures for granting remote only IT access to foreign nationals are described in this NPR (see section 4.10). The policies and procedures necessary to properly manage ICAM services as an integrated end-to-end service to improve security, efficiency, and inter-Center collaboration are covered in NPR 2841.1.

1.2.2 The terms "PIV credential" and "non-PIV credential" are used frequently in this document. The

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

term "PIV credential" refers to the credential which is issued to civil service and contractor employees who need physical or logical access to NASA facilities and IT systems for 180 calendar days or more in a 365-day period. NASA's procedures for issuing PIV credentials must conform to Homeland Security Presidential Directive 12 (HSPD-12). All other credentials issued by NASA are referred to as "Non-PIV" credentials. Non-PIV credentials include such things as: visitor badges, alternate Agency credentials, and other credentials as specified in NPR 2841.1.

1.3 Waivers and Exceptions

1.3.1 Centers might occasionally experience difficulty in meeting specific requirements established in the series of NASA security program NPRs and may request waivers and/or exceptions to those specific requirements. The process for submitting requests for waivers or exceptions to specific elements of the NASA Identity and Credential Management program is as follows:

a. The Asset, Program, or Project Manager and Center Chief of Security (CCS)/Chief of Protective Services (CCPS) shall justify the exception request through security risk analysis: e.g., cost of implementation; effects of potential loss of capability to the Center; compromise of national security information; injury or loss of life; loss of one-of-a-kind capability; or inability to perform its missions and goals, etc.

(1) Justification will also include an explanation of any compensatory security measures implemented in lieu of specific requirements.

(2) The exception request shall be submitted to the Center Director.

b. The Center Director shall confirm that the exception request has the concurrence of both the CCS/CCPS and, as necessary, the Center Chief Information Officer (CIO). The Center Director will then either recommend approval or return the exception request to the CCS/CCPS for further study or closure. The Center Director forwards concurrence to the Mission Support Directorate Associate Administrator at NASA Headquarters.

c. The Mission Support Directorate Associate Administrator shall forward exception requests to the Assistant Administrator (AA) for the Office of Protective Services (OPS) at Headquarters or return proposals to the Center Director for further study or closure. Approval authority of the waiver or exception request resides with the Mission Support Directorate Associate Administrator.

d. The AA for Protective Services will coordinate implementation of any approved waiver or exception for further study or denial and closure.

Chapter 2. Roles and Responsibilities

2.1 Overview

2.1.1 All NASA employees and contractor employees, as well as NASA tenants and contractors for NASA tenants, shall comply with this directive. Government, commercial, educational, or private entities and their employees and contractors (all tiers) needing physical or logical access will also comply with this directive.

2.1.2 The AA for OPS is the system owner of all systems used to manage identities and to issue NASA PIV credentials. The AA for OPS has overall responsibility for ensuring uniformity of credential issuance policies and procedures throughout the Agency.

2.1.3 All NASA organizational components must adhere to the policies and procedures herein and promulgate implementing regulations, as required, consistent with the policies and procedures set forth herein. Center Directors, through their Center OPS, supported by the Center Office of the Chief Information Officer (OCIO), Center Human Resources Office (HRO), Procurement Office, and other offices as necessary will ensure that local operating procedures and execution conform to the policies and procedures herein.

2.1.4 The following roles and responsibilities are established to conform to the guidelines prescribed in National Institute of Standards and Technology (NIST) Special Publication 800-79-1, "Guidelines for the Accreditation of Personal Identity Verification Card Issuers."

2.1.5 Failure to comply with the policies and procedures set forth in this NPR and NPR 2841.1 shall be treated as a violation of security requirements, per NPR 1600.1, section 2.3, and must be reported as a security incident to the CCS/CCPS and the Agency Identity Management Official (AIMO).

2.2 Agency Roles and Responsibilities

2.2.1 Personal Identity Verification (PIV) Card Issuer (PCI) Senior Authorizing Official (SAO) — The AA for OPS shall be the PCI SAO for Identity and Credential Management. The PCI SAO establishes budgets and provides oversight for the identity management and credential management functions and services of NASA. The PCI SAO documents all identity management and credential management responsibilities, roles, and procedures to be followed by NASA. The PCI SAO identifies and designates qualified individuals to the roles of PCI Designated Accreditation Authority (DAA), PCI Assessor, PCI AIMO, and other NASA officials that are involved with Agency identity management. The PCI SAO establishes appropriate attributes and assessment methods for a certification and accreditation, per NIST Special Publication 800-79-1, of the programs and procedures established in this document for the issuance of credentials. The PCI SAO ensures consistent application of this policy across NASA.

2.2.2 PCI AIMO — The PCI AIMO shall be a Federal employee. The PCI AIMO manages the identity management program at NASA and documents the policies and operations of the identity management program in this and other supporting documentation. The PCI AIMO ensures that all personnel, services, facilities, and/or equipment necessary to carry out the policies in this document are procured, updated, and provided reliably. The PCI AIMO ensures that credentials are produced

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

and issued in accordance with the requirements in this document. The PCI AIMO approves all authorizer and investigation reviewer designations. The PCI AIMO recommends and executes an action plan to reduce or eliminate deficiencies and discrepancies identified by the assessor during the certification and accreditation (C&A).

2.2.3 PCI Designated Accreditation Authority (DAA) — The Deputy AA for OPS shall be the PCI DAA. The PCI DAA reviews the certification documentation and the recommendation prepared by the PCI assessor and accredits the PCI as required by Homeland Security Presidential Directive (HSPD)-12. Through accreditation, the DAA accepts responsibility for the operation of the PCI at an acceptable level of risk to NASA. The SAO can also fulfill the role of the DAA.

2.2.4 PCI Assessor — The PCI assessor shall be a Federal employee. The PCI assessor will be organizationally separate from the persons and the office(s) directly responsible for the day-to-day operation of identity management for the Agency and correction of deficiencies and discrepancies identified during the certification. The PCI assessor will have the appropriate skills, resources, and competencies to perform certifications of the Agency. The PCI assessor conducts the PIV C&A, per NIST SP 800-79-1.

2.2.5 NASA Enterprise Applications Competency Center (NEACC) — The NEACC provides hosting and management for core ICAM services. The NEACC provides help desk support for the systems implemented for identity management and credential management including trouble ticket management and procedures for handling escalation. The NEACC formally interfaces with appropriate service, security, support groups, and organizations as required, provides access to technical and user training, computer-based training, and maintains records related to this training.

2.3 Center Roles and Responsibilities

2.3.1 The Center PIV Issuing Facility (PIF) Manager — The Center PIF manager shall be a Federal civil service employee serving as the CCS/CCPS or equivalent role designation at a Center or a designee of the Chief. The PIF manager supports the PCI AIMO at the Center level. The PIF manager oversees the identity management and credential management program implementation at the Center and documents the operations and procedures of the Center's identity management and credential management programs. The PIF manager or designee validates the individuals at the Center who perform the roles of PIV requester and PIV sponsor. The PIF manager or designee monitors training status of all persons fulfilling PIV identity management and credential management roles at the Center. The PIF manager identifies and designates individuals to fill the roles of PIV authorizer, PIV enrollment official, and PIV issuance official. The PIF manager is responsible for ensuring that all personnel, services, facilities, and/or equipment necessary to carry out the policies in this document at the Center are procured, updated, and provided reliably. The PIF manager is responsible for ensuring that credentials are produced and issued in accordance with the requirements in this document. The PIF manager or designee reviews identity source document discrepancies and provides determinations for the acceptance of the documents. The PIF manager or designee is responsible for issuance of all non-PIV credentials (i.e., visitor badges, temporary badges, and alternate Agency credentials).

2.3.2 PIV and non-PIV Applicant — Per Federal Information Processing Standards (FIPS) 201-2, the PIV applicant is the individual to whom a PIV credential needs to be issued. The PIV applicant is a prospective or current NASA worker (e.g., a civil servant or an employee of a Federal contractor), requiring access to NASA facilities and/or IT resources. The PIV applicant is responsible for

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

providing identification documents and data for the PIV request, for being photographed and providing biometrics during enrollment, and providing valid identity documents during enrollment and issuance. The PIV applicant signs for acceptance of the PIV credential and acknowledgement of related responsibilities for proper handling and use of the PIV credential once issued, as defined in Appendix D: Subscriber Agreement of this document. PIV applicants will not perform any role in the creation of their identity and issuance of their credential with the exception of the role of requester for the purpose of renewal and reissuance.

2.3.3 PIV and non-PIV Requestor — The role of PIV requestor is not defined in FIPS 201-2. The PIV requestor is the individual who submits the necessary information on behalf of the PIV applicant to initiate the process of requesting a PIV credential. The non-PIV requestor is the individual who submits the necessary information on behalf of the non-PIV applicant to initiate the process of requesting a non-PIV credential.

2.3.4 PIV and non-PIV Sponsor — The PIV sponsor is defined in FIPS 201-2 as the individual who substantiates the need for a PIV credential to be issued to the PIV applicant and provides sponsorship to the PIV applicant. The PIV sponsor requests the issuance of a PIV credential to the applicant. The PIV sponsor shall be a NASA civil servant employee or a California Technical Institute Jet Propulsion Laboratory employee who establishes and endorses the need for a relationship between the applicant and NASA. The PIV sponsor designates and approves the position risk determination (PRD) in the NASA Identity Management System. The PIV sponsor corrects or completes, as necessary, incorrect or missing information in the credential issuance request. The PIV sponsor is responsible for tracking the status of persons and reporting where access should be modified or terminated. The PIV sponsor is an individual from the identified entity for the following applicant affiliation:

a. Human Resource (HR) specialist for NASA civil service employees.

b. Contracting Officer's Representatives (COR) or other Federal civil service technical personnel responsible for work requirements for contractors.

c. Grants technical official for grantees.

d. Authorizing official or designee for any agreement between NASA and any outside entity.

e. The NASA civil servant program or project manager who requires the foreign national to access NASA facilities or IT systems.

2.3.5 PIV and non-PIV Enrollment Official — The PIV enrollment official covers a portion of the duties that are described in FIPS 201-2 for the PIV registrar. The PIV enrollment official is the entity responsible for identity proofing of the PIV applicant and ensuring the successful collection of the information necessary to confirm employer sponsorship, bind the applicant to their biometric data, and validate the identity source documentation. The role of the PIV enrollment official shall be performed by personnel from the Center Protective Services Office. The PIV enrollment official collects, establishes, and verifies identity information of an applicant. The PIV enrollment official captures the biometrics and photograph of the applicant. The PIV enrollment official checks identity source documents for authenticity, captures copies and/or scans of the identity source documents, compares the name and demographic data in the PIV credential request and the identity source documents, and determines whether any discrepancies exist. The non-PIV enrollment official performs the equivalent functions for non-PIV credentials as the PIV enrollment official does for PIV credentials.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

2.3.6 PIV and non-PIV Authorizer — The PIV authorizer covers the portions of the PIV approval duties described in FIPS 201-2 that are not done by the PIV enrollment official. The PIV authorizer provides the final approval for the issuance of the PIV credential to the applicant. The PIV authorizer and the non-PIV authorizer shall be a NASA civil servant. The PIV authorizer and the non-PIV authorizer will hold no other role in the identity management or credential issuance process for a given identity. The PIV authorizer will hold no role other than the role of applicant in the issuance of their credential. The PIV authorizer and the non-PIV authorizer will be trained in adjudication by an accredited provider of adjudication training. The PIV authorizer reviews the PIV credential request, reviews the PIV sponsor's endorsement, and confirms identity source document validation and biometrics capture has occurred. The PIV authorizer coordinates checks for existing background investigations. The PIV authorizer coordinates requests for background investigations as necessary. The PIV authorizer coordinates background investigation submissions through the OPM Electronic Questionnaire for Investigation Processing (e-QIP), as required. The PIV authorizer adjudicates the results of the fingerprint check and adjudicates background investigation results. The PIV authorizer records the results of the fingerprint check and background investigation results and approves or denies NASA PIV credential issuance. The PIV authorizer records the final result of adjudicated investigations and, when the adjudicated investigations are favorable, authorizes continued use of an issued PIV credential, as required in NPR 1600.3, NASA Personnel Security.

2.3.7 PIV and non-PIV Investigation Reviewer — The PIV investigation reviewer is an optional role within NASA that is not described in FIPS 201-2. The PIV investigation reviewer may be a civil servant or a designated contractor. The PIV investigation reviewer shall not be allowed to authorize production or issuance of a NASA PIV credential. The PIV investigation reviewer assists the PIV authorizer with:

a. Reviewing the PIV credential request, the PIV sponsor's endorsement, and confirming that identity source document validation occurred and that biometrics capture has occurred.

b. Coordinating checks for existing background investigation.

c. Coordinating requests for background investigations, as necessary.

d. Coordinating background investigation submissions through the OPM e-QIP, as required.

e. Reviewing the results of the fingerprint checks and background investigation as they are received.

f. Recording results of the fingerprint check.

g. Updating PIV applicant information when necessary.

2.3.8 PIV and non-PIV Issuance Official — The PIV issuance official is defined in FIPS 201-2 as the PIV issuer. The PIV issuer is the entity that performs credential personalization operations and issues the identity credential to the applicant after all identity proofing, background checks, and related approvals have been completed. The PIV issuance official is also responsible for maintaining records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials. The role of the PIV issuance official shall be performed by personnel authorized by the CCS/CCPS. The PIV issuance official issues NASA PIV credentials to approved PIV applicants. The PIV issuance official is responsible for submitting the order for the PIV credential to be encoded and printed with the appropriate identity information. The PIV issuance official verifies the applicant's identity through visual and biometric verification prior to issuing the NASA PIV credential. The PIV issuance official ensures the applicant has selected a Personal Identification Number (PIN). The PIV issuance official secures, receives, accounts for, and handles unissued

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

NASA PIV credential stock and NASA PIV credentials that are no longer authorized for use due to termination of employment, badge expiration, contract or grant expiration, or expiration of need for the badge by any individual.

2.3.9 PIV Digital Signatory — The PIV digital signatory is the entity that digitally signs the PIV biometrics and Cardholder Unique Identifier (CHUID), as defined in FIPS 201-2.

2.3.10 PIV Authentication Certification Authority (CA) — The PIV Authentication CA is the entity that signs and issues the PIV Authentication Certificate.

2.3.11 International Visit Coordinator (IVC) — The IVC is responsible for reviewing, coordinating, processing, and granting final authorization of all visits, assignments, or access requests by and for foreign nationals visiting NASA. The IVC works with the program managers and sponsors to determine access requirements, work description, dates of the visit, length of the assignment, citizenship, risk associated with the visit, and other pertinent information. The IVC works with the Center Protective Services Office, the program managers, and sponsors to determine escort requirements while the foreign national is located at the Center. Pre-visit identity vetting is conducted and completed by the IVC. The IVC coordinates and ensures access reviews are performed by the following: project office, sponsor, Center Protective Services Office, Center Counterintelligence Special Agent (CISA), and export control office. When necessary, the IVC coordinates review and approval with the Center public affairs office for press or foreign space agency members, the Center protocol office for High-Level Protocol Visits (HLPV), and the Center sponsor and the export control office for NASA Exchange Visitor Program visitors. The IVC informs the sponsor of the approval or denial of the access request and, in the case of approvals, reports the terms and conditions of the visit to the sponsor. The IVC coordinates with request reviewers to ensure appropriate timeframes are followed for processing of the access request and escalates outstanding requests to the AIMO for resolution.

2.3.12 Escort — Escorts are responsible for providing continuous physical supervision of those persons without sufficient access privileges, as determined by a risk-based determination, or need to be granted unsupervised access to the Center/Facility. Escorts of foreign nationals are required to acknowledge understanding and acceptance of the Access Control Plan (ACP) and escort requirements associated with each foreign national visitor, prior to the beginning of the visit. Escorts of foreign nationals are required to maintain active certified escort status by completing annual escort training and maintaining a valid NASA PIV credential, Department of Defense (DoD) Common Access Card (CAC), or other Federal agency PIV that has been successfully registered utilizing the NASA credential registration process. Escorts of foreign nationals are assigned an additional, Agency-standard badge that identifies their certified status as an escort of foreign nationals at that Center/Facility. Escorts of foreign nationals from designated countries are required to complete an in-person briefing with the CISA prior to the visit and an in-person debriefing with the CISA following the visit.

2.3.13 Host — The host is a NASA civil servant or contractor who is the point of contact for detailed information about a foreign national's work requirements and responsibilities. The host understands the technical nature of the visit and works with the sponsor, requestor, and escort to process the individual and ensure they are properly escorted and aware of their responsibilities while at the Center.

2.4 Separation of Duties for the PIV Role

2.4.1 Per the requirements specified in FIPS 201-2, the principle of separation of duties shall be enforced to ensure that no single individual has the capability to issue a PIV credential without the participation of at least one other authorized person.

2.5 Training

2.5.1 Overview training is required for each role identified in this document to ensure a general and uniform understanding of the NASA policies and procedures for identity management.

2.5.2 Role-based training is required for each of the following roles in the PIV issuance process: IVC, PIV enrollment official, PIV authorizer, PIV investigation reviewer, and PIV issuance official. Recertification is required each year to ensure training is up-to-date and conducted with the most recent system updates. Failure to complete annual recertification will result in the individual's role being revoked. Training records are maintained by the System for Administration, Training, and Educational Resources for NASA (SATERN) computer-based training system or subsequent/succeeding system(s).

2.6 Privacy

2.6.1 NASA shall ensure that applicant information and systems which facilitate identity management processes are managed consistent with:

a. NPD 1382.17, NASA Privacy Policy.

b. NPR 1382.1, NASA Privacy Procedural Requirements.

c. Homeland Security Presidential Directive 12 (HSPD-12).

d. OMB Memorandum 05-24.

e. Privacy Act of 1974 (Public Law 93-579, 5 U.S.C. § 552a).

f. E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. § 101).

2.6.2 As prescribed in NPR 1382.1, NASA shall conduct and maintain a Privacy Impact Assessment (PIA) of the identity management program. NASA will conduct and maintain PIAs for all systems which are used in the identity management processes and include Personally Identifiable Information (PII) and Information in Identifiable Form (IIF) of the applicant. The NASA System of Records Notice (SORN) will be updated and maintained to reflect the disclosure of information to other Federal agencies.

2.6.3 Only individuals with a legitimate need to access the systems in which an applicant's IIF is stored and maintained shall be allowed to access those systems. It is the responsibility of each Center PIF manager to ensure that the access restrictions defined in the PIA are enforced. NASA will ensure privacy of applicant information is sustained through all steps of identity management including enrollment and issuance. PIV credential issuance facilities will provide an electromagnetically opaque sleeve that assists in protecting against unauthorized contactless access to information stored in the PIV credential.

2.6.4 The Privacy Act Statement shall be posted in every enrollment and issuance location, on the applicable NASA Web site, and provided in pre-enrollment packages to the applicant. The Privacy

Act statement covers:

a. Use of collected PII.

b. Protections provided to ensure the security of PII.

c. Effects of partial disclosure and non-disclosure of information by the applicant.

2.6.5 The Subscriber Agreement (see Appendix D: Subscriber Agreement) shall be posted in every enrollment and issuance location on the applicable NASA Web site and provided in any pre-enrollment packages to the applicant. The Subscriber Agreement covers:

a. Authorized uses of the PIV credential.

b. Authorized uses of the Public Key Infrastructure (PKI) certificates and services provided with the PIV credential.

c. Notification requirements for the applicant.

d. Requirements to return the PIV credential at the end of use.

2.6.6 The following documentation shall be made available, at the request of the applicant:

a. Complaint procedures.

b. Appeals procedures, as described in NPR 1600.3, for those denied a PIV credential or whose PIV credential is revoked.

c. Consequences for employees violating NASA privacy policies, as described in NPR 1382.1.

2.6.7 All notifications provided during identity management processes shall be conducted in a secure manner, ensuring applicant information is secure at all times. Centers will establish procedures for notifying applicants when their PII is lost, damaged, becomes corrupt, or stolen.

2.6.8 Any individuals violating the privacy requirements established in this chapter may be disciplined and/or banned from physical or logical access in compliance with NASA guidelines established in NPR 1382.1.

2.6.9 NASA shall archive and safeguard all stored data pursuant to NPD 1440.6, NASA Records Management, and NPR 1441.1, NASA Records Retention Schedules. Identity files are maintained for a minimum of two years after an individual's relationship with the Agency has ended. NASA may, at its discretion, increase but not reduce the time that identity source documents are to be maintained. The data to be maintained in electronic or hard copy includes:

a. Completed and signed PIV credential request.

b. Information related to the applicant's identity source documents.

c. Results of the applicant's background check.

d. Copies of the applicant's photograph.

e. Any additional documents used in the enrollment and issuance process.

Chapter 3. Enrollment and Credential Issuance

3.1 Overview

3.1.1 The NASA Identity Management and Credential Management Processes are designed to conform to the system-based model for identity proofing, registration, and issuance process that is described in NIST FIPS 201-2.

3.1.2 The NASA Identity Management and Account Exchange (IdMAX) system shall be the sole and authoritative source for the enrollment and processing of NASA identity data, as recognized by the Office of Management and Budget (OMB), per the Paperwork Reduction Act (OMB control number 2700-0158), and for the processing of access requests and for the issuance of credentials.

3.2 Chain of Trust

3.2.1 A chain of trust is followed which simultaneously captures the biometrics, photograph, identity source documents, and background investigation of the applicant and can be tied to the identity of that applicant at any point in the identity management process.

3.2.2 The credential is released to the applicant only after completion of the chain of trust by verifying that the biometric information contained on the credential matches the applicant.

3.3 NASA Credential Types

3.3.1 NASA uses both PIV credentials and non-PIV credentials. Each NASA credential is linked to an established identity and shall go through the appropriate issuance steps as outlined in this chapter. See NPR 2841.1, for policy and procedures regarding NASA non-PIV credentials that allow access to only logical systems. Requirements for the characteristics of these credentials, including printing elements and technology capabilities are detailed in Chapter 5, Characteristics of NASA Badges.

3.3.2 NASA PIV Credentials

3.3.2.1 NASA PIV credentials shall be required for all persons who have been deemed as needing routine and regular physical only, logical only, and/or both physical and logical access to NASA Centers, facilities, and IT systems and resources for a period exceeding 179 calendar days in a 365-day period. These persons include all NASA employees, all NASA contractors, agreement partners, and non-NASA tenants in NASA facilities. NASA PIV credentials will be issued to both United States (U.S.) citizens and foreign nationals.

3.3.2.2 NASA PIV credentials will be issued following the identity proofing, registration, and issuance processes defined in this document for the management of identities of all new and current employees, contractors, and affiliates including foreign nationals.

3.3.2.3 NASA PIV credentials will be issued only after completion of a Federal Bureau of Investigation (FBI) fingerprint check and submission of a background investigation, which will be a Tier I background investigation, at a minimum.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

3.3.2.4 NASA PIV credentials will have an expiration date set for a period not to exceed five years from the Card Production Request (CPR) generation date.

3.3.2.5 NASA PIV credentials shall not be issued to individuals holding a Federal PIV credential issued by another Federal entity. Reserve military personnel who are full-time NASA employees or contractors are exempt from this restriction and may be issued a NASA PIV credential in addition to their DoD CAC. Exceptions to this policy may be made only when the exception has been documented and approved via the process described in section 1.3, Waivers and Exceptions, of this document. The exception request will specifically explain why a non-NASA credential is not usable in the NASA ICAM services.

3.3.3 NASA Non-PIV Credentials

3.3.3.1 All NASA non-PIV physical access credentials shall be created utilizing the Agency Enterprise Physical Access Control System (EPACS) and in compliance with NPR 2810.1.

3.3.3.2 NASA non-PIV temporary credentials will be issued to any person (e.g., NASA employee, NASA contract personnel, non-NASA tenant, or other category of individuals; such as volunteers, guest researchers, interns, grantees, etc.) who needs access to a NASA facility or NASA IT system and who will be affiliated with NASA and its Centers or facilities for a period of less than 180 calendar days (up to 179 calendar days) in a 365-day period. The 180-day period begins the first day of affiliation and ends 179 calendar days later regardless of the work schedule. If an individual's affiliation extends for 180 calendar days in a 365-day period from the first day of affiliation regardless of the work schedule, the individual will be issued a NASA PIV credential. The following categories of affiliates with no logical access may, at the discretion of the CCS/CCPS, be exempted from the requirement to receive a NASA PIV credential at the 180 calendar day point: seasonal student interns, volunteers, construction workers, and others as approved by the AIMO.

3.3.3.3 Issuance of NASA non-PIV badges requires a minimum favorable adjudication of a National Crime Information Center (NCIC) name query and completion of steps 1-4 of section 3.5, On-Site Enrollment and Issuance Procedures for NASA Credentials, of this NPR. Escort requirements for individuals with a NASA non-PIV badge will be based on risk-determination by the CCS/CCPS, in compliance with the requirements in this document.

3.3.3.4 NASA non-PIV visitor badges allow physical-only access to the issuing NASA Center. For visitors, Centers are authorized to issue alternate agency credentials (i.e., NASA non-PIV credentials) for physical access to that Center based on a risk-based determination documented as part of the permanent record. NASA visitor badges shall be issued to individuals requiring access to a NASA Center for a period less than 30 calendar days in any single visit and not more than a cumulative total of 29 calendar days in a 365-day period. Escort requirements for individuals with visitor badges will be based on risk-determination by the CCS/CCPS, in compliance with the requirements in this document.

3.3.3.5 NASA non-PIV alternate Agency credentials shall be issued to accommodate unique situations of the Center not otherwise accommodated by NASA PIV credentials and NASA visitor badges. All NASA alternate Agency credential templates will have the approval of the Agency Identity Management Official prior to their creation and utilization. NASA alternate Agency credentials will be issued upon completion of a favorable adjudication of an NCIC name query. This is a minimum requirement, and additional security measures may be employed at the discretion of the CCS/CCPS. Issuance of these credentials will be based on a risk-based access determination by the CCS/CCPS. NASA alternate Agency credentials may be issued to individuals who hold a PIV

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

credential issued by another Federal Government agency or department if their current non-NASA PIV credential does not work at the NASA Center. This may include contractors from another NASA Center in the event that electronic verification of a requirement to access the NASA Center is not available at a point of entry. Issuance of alternate Agency credentials requires completion of steps 1-3 of section 3.5, On-Site Enrollment and Issuance Procedures for NASA Credentials, verification of a favorably adjudicated investigation, and capture of the individual's photograph.

3.3.4 Logical-only access credentials and their usage are addressed by NPR 2810.1 and include, but are not limited to, username and password, RSA tokens, and digital certificates.

3.4 Applicant Categories

3.4.1 NASA employees are Federal civil servants employed and paid by NASA and also includes individuals employed and paid by other entities but working for NASA under an Intergovernmental Personnel Act (IPA) agreement. NASA employees include all Non-Appropriated Funds Instrumentality (NAFI) employees; these employees shall be issued a civil servant badge with the affiliation of NAFI.

3.4.2 NASA contractor employees are individuals working for a contracting organization or entity with the responsibility to perform activities for NASA.

3.4.3 NASA grantees are individuals who are working under a grant or cooperative agreement and performing grant-funded activities at NASA Centers and facilities.

3.4.4 Detailees, for the purposes of this NPR, are either Federal employees from other-Federal agencies, U.S. military personnel, or non-Federal employees working at NASA through an IPA assignment. Any badges issued to a detailee shall be designated with an affiliation of NASA and will appear as a Federal employee badge. The Center PIF manager will coordinate with the Center HRO to validate investigative and suitability results for detailees from other-agency partners. Government employees from other departments and agencies who do not have a PIV credential issued by their agency or department and require identity verification and access at NASA may be issued a NASA PIV credential or NASA alternate Agency credential.

3.4.5 International partners are individuals working for agencies or organizations of foreign governments, foreign education institutions, foreign companies, or international organizations who are engaged in a program of international cooperation in work done pursuant to a Space Act Agreement, as defined by NPD 1050.1, Authority to Enter into Space Act Agreements. A signed international agreement shall first be in effect for international partners to receive a foreign national NASA PIV credential.

3.4.6 Tenants are individuals who require physical access to a NASA facility but may not work directly for NASA, including individuals requiring access under any property agreement (e.g., Enhanced Use Lease) with NASA. There may or may not be a "formal" agreement associated with a tenant (e.g., Credit Union). The tenant may require logical access to certain NASA applications. A tenant may work for another Government agency as either a civil servant or contractor and may have a PIV badge from their agency. Tenants shall be issued alternate Agency credentials. Tenants without a PIV badge from another Government agency may, at the discretion of the CCS/CCPS, be issued NASA PIV badges following the processes and requirements for a NASA PIV badge. Tenants with a PIV credential from another Government agency which cannot be registered in IdMAX may be issued alternate Agency credentials (non-PIV), at the discretion of the CCS/CCPS.

3.4.7 Transients are individuals (i.e., construction workers, club members, childcare drop off/pickup, delivery drivers, retirees, Center transits, and others requested by CCS/CCPS and approved by the AIMO) who requires intermittent access for 180 calendar days or more. Transients shall be issued alternate Agency credentials.

3.4.8 Interns are students from educational institutions participating in NASA internship/research programs and programs or projects which benefit and/or further the goals, objectives, and efforts of NASA.

3.5 On-Site Enrollment and Issuance Procedures for NASA Credentials

3.5.1 Step 1: Credential Request

3.5.1.1 A requester completes a credential request within the NASA Identity Management System for an applicant. The requester submits the request to the sponsor via the NASA Identity Management System. For civil servants, this information is submitted by the HRO via Workforce Transformation Tracking System (WTTS). The information submitted includes the following:

a. Name of the applicant.

b. Date of birth of the applicant.

c. Home address.

d. Social Security Number (SSN).

e. Position of the applicant.

f. Contact information for the applicant.

g. Name of the requester.

h. Organization of the requester.

i. Contact information for the requester.

3.5.2 Step 2: Sponsorship.

3.5.2.1 The sponsor validates the receipt of the request from the requester and reviews the data in the request. The sponsor reviews the Position Risk Determination in the NASA Identity Management System and approves or denies the request, establishing the need for a relationship between the applicant and NASA and the applicant's need for a PIV credential.

3.5.3 Step 3: Check for Background Investigation or Database Checks.

3.5.3.1 The authorizer or investigation reviewer validates the receipt of the request from the sponsor. The authorizer and supporting staff review OPM and other Federal databases and take appropriate steps to validate the applicant's investigation status with regard to a current investigation.

3.5.3.2 If the applicant has an investigation on file or in progress that meets the investigative and reciprocity requirements, the authorizer submits the request to the enrollment official and the

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

applicant proceeds to enrollment, section 3.5.4, Step 4: Enrollment Process for capture of enrollment data with flat fingerprints.

3.5.3.3 If no investigation is on file or in progress, the authorizer coordinates initiation of an invitation in the OPM e-QIP for the applicant to complete the appropriate background investigation form and authorizes the enrollment official to obtain the applicant's flat and rolled fingerprints, identity source documents, and photograph.

3.5.3.4 If the applicant is requesting a non-PIV alternate Agency credential then the authorizer or designee conducts the appropriate database checks and approves the credential if the database checks are favorable. The submission of the captured fingerprints to OPM is optional, as determined by the CCS/CCPS.

3.5.4 Step 4: Enrollment Process.

3.5.4.1 The enrollment official validates the receipt of the request from the authorizer. The sponsor advises the applicant that they will appear in person before the enrollment official and present two forms of identity source documents in original form. The applicant then appears in person before the authorized enrollment official and presents two forms of NASA-approved identity source documents in original form, one of which will be a Federal or state issued picture identification. The enrollment official inspects the source document for authenticity and validates the source document through visual or electronic scrutiny and, when necessary, with the authority or entity which issued it.

3.5.4.2 Enrollment Fingerprints — The applicant's fingerprints are captured. If the applicant currently has a favorable background investigation on file or in progress, only flat fingerprints are required. If no background investigation is on file or in progress, both flat and rolled fingerprints are required. In cases where there is difficulty in collecting fingerprints due to damage, injury, or deformity, NASA will process the credential with a designation of fingerprints as non-classifiable. The facial image collected from the applicant during enrollment can also be used for authenticating badge recipients covered under Section 508 of the Rehabilitation Act.

3.5.4.2.1 When fingerprints are captured at a location other than the Center Protective Services Office, the transmission of those fingerprints to the Center Protective Services Office shall be from a valid law enforcement agency or other accredited fingerprint provider. To ensure a chain of trust, the fingerprint cards will be delivered to the Center Protective Services Office by the entity that took the fingerprints.

3.5.4.3 Enrollment Photograph — The applicant's photograph is captured which will include the entire face, from natural hairline to the chin, and may not be obscured by dark glasses, hats, etc. The facial expression shall be neutral (non-smiling) with a closed mouth. Eye patches that do not obscure an excessive portion of the face need not be removed. Individuals with temporary eye patches should be issued a temporary badge until such time when the patch is no longer necessary and an unobscured, full-facial photograph can be captured. Waivers for religious reasons may be obtained by written application to the AA for OPS.

3.5.4.4 NASA-Approved Identity Source Documents — The enrollment official obtains and maintains legible photocopies or scanned copies of the original identity source documents. Any documents that appear invalid (e.g., absence of security hologram or other known security features on a state issued driver's license, security features on a birth certificate or passport, smeared ink, etc.) are to be rejected by the enrollment official and reported to the proper authority for review.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

Photocopies of rejected documents are to be made and retained for a period not to exceed one year or until any appeal process is completed. Identity source documents that do not pass electronic examination are rejected and another approved identity source document will be obtained and subjected to electronic scrutiny. In the event the applicant is required to provide documentation to resolve discrepancies or omissions in data collected, the enrollment official shall review the information with the applicant as necessary. The information submitted by the applicant will be used to update the applicant identity record.

3.5.4.5 Enrollment Subscriber Agreement — For applicants requesting PIV credentials, the enrollment official shall provide the applicant with the Subscriber Agreement, (See Appendix D: Subscriber Agreement), and obtain an electronic signature of the applicant attesting to their reading and acceptance of the Subscriber Agreement.

3.5.5 Step 5: Adjudication Process.

3.5.5.1 If no investigation is on file or in progress, the fingerprints captured during enrollment shall be submitted to OPM with a request for a background investigation. The authorizer receives the results of the fingerprint check. If the fingerprint check comes back with a status of unclassifiable, the Center will use the results of a name check to process the PIV credential request. The authorizer makes a determination based upon receipt of the fingerprint check results or evidence of an acceptable existing background investigation (as found in section 3.5.3, Step 3: Check for Background Investigation or Database Checks), if the applicant is eligible to receive a PIV credential. If the adjudication of the available background investigation is favorable, the authorizer will submit a PIV credential issuance request to authorize the creation and issuance of a PIV credential. Final adjudication of the record is performed in compliance with NASA personnel security policies.

3.5.6 Step 6: Badge Production Process.

3.5.6.1 The PIV authorizer submits a request for badge printing if the badge is to be printed remotely at a commercial facility or a shared service provider. The necessary information is included in a batch card creation request. The initialized and printed badges are returned to NASA and forwarded to the appropriate issuance officials where the credentials shall be held in a secure location. If the badge is to be produced locally, the issuance official will print the identity information onto the card and compare the photo to the identity database. The badge will be encoded with the identity and biometric data of the applicant. The encoded badge will be tested, and the applicant will be notified when the badge has been successfully encoded.

3.5.7 Step 7: Issuance Process.

3.5.7.1 The applicant appears before the issuance official, who establishes whether the badge was printed in a batch job, previously printed on-site, or is to be printed on-site. If the badge is printed in a batch job or previously printed on-site, the issuance official will obtain the card stock from storage. If the badge is to be printed on-site, the issuance official will obtain a blank badge from storage, verify the identity of the applicant against the database, and print the badge. The issuance official checks the printed badge to verify the identity of the applicant, conducts a biometric match, and encodes the badge with an applicant entered PIN number. Upon completion of the badge printing and encoding, the badge is officially released to the applicant. An approved electronically shielded badge holder shall be offered to the applicant in order to protect the badge and the privacy of information on the badge.

3.5.7.2 For any badge issued without a biometric check, facial recognition shall be performed by comparing the photograph stored in IdMAX to the photograph on the badge and the face of the applicant. When the facial recognition is verified, the badge can be released to the applicant.

Chapter 4. Foreign Nationals

4.1 Overview

4.1.1 This chapter outlines the requirements that NASA personnel shall follow in granting access to foreign nationals to NASA physical and/or IT resources for any purpose other than an appropriately authorized tour of facilities that is, or would normally be, conducted for the general public. The subsections outline additions and variations to existing processes, procedures, and authorizations necessary to successfully obtain required access permissions in a timely manner. Also included are the requirements for the processing of persons who have multiple citizenships, foreign nationals from designated countries, Lawful Permanent Residents (LPR), and U.S. citizens working for a foreign entity.

4.1.2 This chapter defines the identity management requirements specific to foreign nationals at NASA including, but not limited to, visit coordination, access approval, escort procedures, fingerprint checks, and background investigations for permanent, temporary, and visitor access.

4.1.3 The requirements in this chapter apply to all foreign nationals, including but not limited to foreign nationals who are civil servants, contractors, researchers, international partners as defined via International Space Act Agreements (ISAA), HLPV, foreign nationals with the news media, NASA-sponsored J-1 Visas, grantees, and visitors.

4.1.4 Questions regarding the receipt and processing of access requests for foreign nationals and the conduct of approved visits and other access shall be directed to the NASA Center or Component Facility IVC. If the criteria for processing a specific foreign national cannot be accommodated within one of the scenarios documented in this chapter, a waiver request can be submitted to the NASA OPS for review and approval (see section 1.3, Waivers and Exceptions of this document).

4.2 NASA Foreign National Access Policy and Related Requirements

4.2.1 Foreign national access is determined on a case-by-case basis. All visits and other approved access will be reviewed to ensure the request conforms to Agency and Federal policies and regulations, including U.S. national security, export control, nonproliferation, and foreign policies and regulations.

4.2.2 Record keeping related to tracking foreign national access requests and visits will be accomplished via the NASA IdMAX system.

4.2.3 Visits and other access for the purpose of implementing a mutually agreed upon program or project shall comply with the terms of the NASA/foreign partner program or project agreement, particularly the provisions in the agreement dealing with responsibilities of the parties and the transfer of data and goods. Discussion or other release of information by NASA personnel to a foreign national during a visit or other approved access that does not pertain to an agreed program or project will be limited to information releasable to the general public, i.e., unclassified, non-sensitive, and non-export controlled. Scientific and Technical Information (STI) that is proposed for release outside of NASA is required to be reviewed in order to ensure it does not contain

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

sensitive information, including Sensitive But Unclassified (SBU)/Controlled Unclassified Information (CUI), per NPR 2200.2, Requirements for Documentation, Approval, and Dissemination of NASA Scientific and Technical Information.

4.2.4 Visits, assignments, or IT access requests for foreign nationals from nondesignated countries are coordinated and implemented at the Center level through the IVC. Visits, assignments, or IT access requests for foreign nationals from designated countries are coordinated initially through the Center Export Administrator (CEA) and the Center IVC, then forwarded to NASA Headquarters Office of International and Interagency Relations (OIIR), Export Control Administrator, and program points-of-contact, as necessary, for review and final approval. A foreign national will be provided access to NASA physical and/or IT assets only after final approval. For a current list of designated countries, refer to the OIIR Web page at: http://oiir.hq.nasa.gov/nasaecp.

4.2.5 An approved foreign national visit request will allow access to information that is releasable to the general public. Visit requests with the purpose of gathering or sharing information or conducting discussions in areas that NASA considers sensitive (e.g., for proprietary, national security, or export control reasons) shall be disapproved in the absence of a specific NASA programmatic interest.

4.2.6 All foreign national access requests, other than for an authorized public tour coordinated through a NASA visitor center, shall undergo an identity vetting and credentialing process in accordance with this chapter.

4.2.7 Foreign national identities and associated access permissions shall be suspended on the day the foreign national's affiliation ends.

4.2.8 Identities and access permissions shall be terminated the day the affiliation ends for foreign nationals from designated countries and 30 calendar days after affiliation ends for foreign nationals from nondesignated countries.

4.2.9 Access shall only be granted to vetted foreign nationals from designated and nondesignated countries consistent with the completed Access Control Plan (ACP), as defined by NPR 2190.1, NASA Export Control Program.

4.2.10 Physical access permissions are granted by the Center Protective Services Office. IT access permissions are granted by IT system owners. The decision to grant physical and/or logical access to foreign nationals to NASA's restricted areas, mission essential infrastructure, sensitive or classified information, and/or export-controlled data may require a higher level of identity vetting due to the heightened risk of exposing these areas and data.

4.2.11 Access requirements established by this NPR shall not preclude each Center Protective Services Office from enacting additional requirements regarding access to the Center, buildings, or other secured areas.

4.2.12 Escort Requirements

4.2.12.1 The IVC shall work with the Center Protective Services Office, CEA, program managers, and sponsor to determine escort requirements while the foreign national is located at the Center.

4.2.12.2 The escort and foreign national shall acknowledge understanding and acceptance of the ACP and the associated escort requirements.

4.2.12.3 The Center Protective Services Office shall be responsible for developing and conducting training for all escorts.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

4.2.12.4 Centers shall determine the necessary escort-to-visitor ratio for foreign nationals from nondesignated countries.

4.2.12.5 Foreign nationals from designated countries shall be escorted at all times.

4.2.12.6 One escort shall be assigned to each foreign national from a designated country so that an escort-to-visitor ratio of 1:1 is maintained. For High-Level Protocol Visits (HLPV), Centers may determine a different escort-to-visitor ratio.

4.2.12.7 Escorts of foreign nationals shall maintain continuous physical supervision of their assigned visitor for the entire duration of the visit, beginning with the visitor's initial entry through the Center perimeter and concluding with the visitor's final exit through the Center perimeter.

4.2.12.8 Escorts shall only permit access to areas which the escort and the visitor have been granted access.

4.2.12.9 Per NPR 1660.1, NASA Counterintelligence and Counterterrorism, escorts of foreign nationals from designated countries shall complete an in-person briefing with a Center CISA prior to the visit as well as an in-person debriefing with a Center CISA following the visit.

4.2.12.10 Escorts of foreign nationals shall be given an additional, Agency-standard badge that identifies their certified status as an escort of foreign nationals at that Center/Facility. This badge must be clearly displayed at all times while escorting foreign nationals.

4.2.12.11 Only trained escorts who are U.S. citizens, LPRs, or foreign nationals from nondesignated countries with a valid NASA PIV credential, or a Department of Defense Common Access Card (CAC) or other Federal agency PIV that has been successfully registered utilizing the NASA credential registration process, shall be allowed to escort foreign nationals.

4.2.12.12 Foreign nationals from designated countries shall not be allowed to perform duties as an escort.

4.2.13 Escorts of all foreign nationals, from both designated and nondesignated countries, shall complete annual training which includes the following information:

4.2.13.1 The requirements to become an escort and maintain escort status, as detailed in this section.

4.2.13.2 The roles and responsibilities of escorting foreign national visitors on a NASA Center/Facility including maintaining continuous physical supervision of the foreign national visitor at all times, Center-specific escort policies, and the duration of escort responsibilities beginning at initial visitor entry through the Center perimeter and concluding at final visitor exit through the Center perimeter.

4.2.13.3 Explanation of an ACP, its requirements, and mandated adherence.

4.2.13.4 Limitations/restrictions associated with where escorts can take foreign national visitors (i.e., only to areas where both escort and visitor have been granted access).

4.2.13.5 The requirement to report to CCS/CCPS any violations or suspected violations of the ACP or visitor policies.

4.2.13.6 Ratios for escort-to-foreign national visitors from designated and nondesignated countries.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

4.2.13.7 The requirement to participate in in-person briefings and debriefings with the Center CISA prior to and following escort of foreign nationals from designated countries.

4.2.13.8 Signed acknowledgement, in SATERN, of escort roles and responsibilities at the completion of escort training.

4.2.14 Escorts of foreign nationals from designated countries shall complete in-person briefings with the Center CISA prior to each visit, per NPR 1660.1, which includes the following information:

4.2.14.1 Explanations and examples of information gathering techniques.

4.2.14.2 Information specific to the designated country, such as the types of technology or information that the designated country is interested in obtaining.

4.2.14.3 Project-specific information that must be protected.

4.2.14.4 The requirement to report to CCS/CCPS and the Center CISA any violations or suspected violations of the ACP or visitor policies.

4.2.14.5 The requirement for the escort to attend an in-person debriefing with the Center CISA following each visit.

4.2.14.6 Written acknowledgment of the receipt of the briefing and debriefing for escorts of foreign nationals from designated countries.

4.2.15 Requests to Visit Another Center.

4.2.15.1 Foreign nationals with PIV credentials shall be granted access to their primary Center only.

4.2.15.2 Access to Centers other than the primary Center shall not be allowed until a Visiting Center Request has been completed in IdMAX and the request has been reviewed. Requests for access will only be granted to physical and logical assets listed in the ACP and the NASA Access Management System (NAMS). Physical access is at the discretion of the CCS/CCPS.

4.2.16 Centers and/or programs may specify restrictions regarding physical and/or logical access privileges or escort requirements that are more restrictive than those documented in this NPR.

4.2.17 Any violation or suspected violation of the ACP or visitor policies shall be reported to the CCS/CCPS and the CEA.

4.3 On-Site Enrollment and Issuance Procedures for Foreign Nationals

4.3.1 Foreign nationals shall complete the following steps prior to initiation of any on-site enrollment and issuance procedures:

a. Obtain visit approval for the visit or assignment.

b. Obtain a visa sufficient for the purpose of the visit or assignment.

c. Be responsible for ensuring that sponsorship is determined. If a foreign national is not under a contract where a COR has been officially designated, the foreign national will provide information directly to their visit/assignment host, and the host will fulfill the duties of the sponsor as required herein.

d. The foreign national visitor must begin the process long enough before the visit so that pre-visit identity vetting can be conducted and completed by the IVC, as described in this chapter.

4.3.2 Step 1: Credential Request.

4.3.2.1 The requester for a foreign national shall be a current PIV holder. The requester submits the following information to the sponsor via the IdMAX system:

a. Full legal name.

b. Date of birth.

c. Place of birth.

d. Residence (including country).

e. Citizenship(s).

f. Passport and visa information (including appropriate visa waiver as found in section 4.6, Requirements for Visas).

g. SSN (if one is available).

h. Foreign national ID (if no SSN is available).

i. Contact information.

j. Company of employment.

k. Sponsor name.

l. Physical access requirements.

m. IT access requirements (on-site and/or remote).

n. Data access requirements (including export control license or authorization requirements).

o. NASA affiliation (civil servant, contractor, partner, etc.).

p. Visit duration.

q. Work description (includes purpose, program, authority, or other information that allows approvers to make an informed decision). The more information provided, the quicker the request can be processed.

4.3.3 Step 2: Sponsorship.

4.3.3.1 The sponsor will be a NASA civil servant or a JPL California Institute of Technology (Caltech) employee who is a U.S. citizen. The sponsor validates the receipt of the request from the requester, reviews the data in the request, and updates the data as necessary. The sponsor will perform a risk-based determination based on the status of the foreign national and the assets that the foreign national is to access. This information is necessary to define the ACP and determine the level of investigation and escort requirements.

4.3.3.2 A foreign national must be assigned a primary Center. If a foreign national will be accessing

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

multiple Centers, access must be granted through a Visiting Center Request in IdMAX (as detailed in section 4.2.15, Requests to Visit Another Center).

4.3.4 Step 3: Foreign National Approval.

4.3.4.1 The IVC shall directly receive and review all access requests for foreign nationals. The IVC validates receipt of the request and confirms sponsorship of the request. The IVC performs or ensures completion of the following reviews and activities, in any order, prior to final approval and authorization, as appropriate.

4.3.4.2 Access Request Review — The IVC reviews the access request with the project office (requesting organization) and the sponsor to confirm access requirements, work description, dates of visit, assignment or length of access request, visa type and its appropriateness to the assignment and visit duration, sponsor's risk determination, and the ACP. The request shall be approved or rejected, as appropriate.

4.3.4.3 Identity Vetting — The IVC performs checks against appropriate databases, in accordance with the identity vetting requirements in section 4.5, Identity Vetting Requirements.

4.3.4.4 Security Review — The IVC reviews the access request within the Center Protective Services Office for broader security issues relevant to the Center, determines escort requirements, reviews the ACP, and approves or denies the request, as appropriate. If approved, a level of investigation appropriate to physical and/or IT access requirements, visit type, and length of residence in the U.S. is determined and initiated.

4.3.4.5 Counterintelligence/Counterterrorism Review — Center and HQ CISAs perform name checks for foreign nationals of interest to determine intelligence service and/or terrorism affiliations.

4.3.4.6 Export Control Review — Export control issues are reviewed by the CEA to ensure information being exchanged does not violate export control laws. Further review is conducted by Headquarters Export Control if the foreign national is from a designated country, an intern, or part of the NASA Exchange Visitor Program. A risk-based determination on access protocols is made, the ACP is reviewed, and the request is approved or denied, as appropriate.

4.3.5 Step 4: Authorization.

4.3.5.1 The IVC shall confirm receipt of all approvals and reviews and provide final authorization of the access request.

4.3.5.2 The IVC shall report the terms and conditions of the visit, as contained in the ACP, to the sponsor.

4.3.5.3 If a foreign national is denied access (all or in part), the IVC shall inform the sponsor who may request a further review with the CCS/CCPS.

4.3.6 Step 5: Enrollment Process.

4.3.6.1 The enrollment official validates receipt of the request from the authorizer and follows the enrollment procedures in section 3.5.4, Step 4: Enrollment Process, with the following variation:

4.3.6.2 Visit Authorization Documents — The enrollment official obtains legible scanned copies of the following original documents:

a. Visa or Electronic System for Travel Authorization (ESTA) receipt for visa waivers.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

b. Admission stamp or paper Form I-94, Arrival/Departure Record, with Admitted-Until Date or "D/S" (duration of status).

4.3.7 Step 6: Adjudication.

4.3.7.1 Adjudication follows the adjudication procedures in section 3.5.5, Step 5: Adjudication Process, of this NPR, in accordance with the identity vetting requirements in section 4.5, Identity Vetting Requirements.

4.3.8 Step 7: Credential Production and Issuance.

4.3.8.1 Credential production and issuance follow the procedures described in sections 3.5.6, Step 6: Badge Production Process, and 3.5.7, Step 7: Issuance Process, of this NPR.

4.3.9 Step 8: NAMS Access Request.

4.3.9.1 If accessing NASA IT resources, access requests will be reviewed by the system owner/approver who shall approve the request in NAMS, as appropriate.

4.4 Implementation

4.4.1 The sponsor and/or host shall ensure the foreign national understands and accepts the terms and conditions of the visit, as contained in the ACP.

4.4.2 The sponsor, supported by the host and escort, shall ensure the foreign national adheres to the access requirements documented in the ACP throughout the duration of the foreign national's affiliation.

4.4.3 If a foreign national application has been outstanding for longer than 15 working days from the initial request, the IVC shall follow up with Center or Headquarters personnel to determine the cause(s) for the delay. Applications outstanding for longer than 20 working days from the initial request will be escalated to the AIMO for resolution.

4.5 Identity Vetting Requirements

4.5.1 Centers shall accept as valid the identity vetting of their peer Centers as a baseline requirement, consistent with this NPR. Additional identity vetting may be required should access requirements change (e.g., if the foreign national needs privileged access).

4.5.2 For foreign national visits of 29 calendar days or less (short-term) which require no IT access, the following shall be required:

a. A visual compliance database check that reveals no violations or derogatory information;

b. FBI Investigations File (name check search).

c. A database check of the U.S. Customs and Immigration Service (USCIS) Systematic Alien Verification for Entitlements (SAVE) to confirm reciprocity of vetting performed by Customs and Border Patrol at the port of entry.

4.5.3 For foreign national visits of 30 calendar days or greater (long-term) or when IT access is

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

required, the foreign national shall be subject to the following database checks prior to the issuance of any credential:

a. FBI fingerprint-based national criminal history check (NCHC).

b. FBI Investigations File (name check search).

c. USCIS SAVE.

d. Visual Compliance, which includes a check against the Visual Compliance Unverified List, Entities List, Denied Persons List, Debarred Parties List, Specially Designated Nationals, and the Terrorist Screening database.

4.5.4 Access requests for foreign nationals shall be denied if the NCHC or Visual Compliance check produces any positive hit result showing the specific individual on any available list in Visual Compliance. Positive hit results are to be reported to the CCS/CCPS and the NASA Headquarters Export Control Administrator. Exceptions to this denial of access are granted in cases where the positive result can be effectively mitigated by an applicable ACP proviso approved by the NASA Headquarters Export Control Administrator.

4.5.5 Access requests for foreign nationals shall be denied if the SAVE check verification process reports an invalid immigration status.

4.5.6 Foreign nationals requiring a PIV shall be subject to investigation based on their time of residence in the United States.

4.5.6.1 For foreign nationals who have resided in the U.S. or a U.S. territory for three years or more, a background investigation (i.e., Tier I background investigation or higher) will be initiated after employment authorization is appropriately verified. Foreign nationals are eligible for issuance of a NASA PIV credential upon favorable adjudication of a Tier I investigation or higher. In the event a foreign national chooses not to complete the appropriate forms for a background investigation required for full identity vetting, the Center Protective Services Office will require completion and a minimum annual revalidation of the NCHC, FBI Investigations File, Visual Compliance, and SAVE checks prior to issuance of an alternate Agency credential.

4.5.6.2 For foreign nationals who have resided in the U.S. or a U.S. territory for less than three years, the background investigation shall be delayed until the three-year requirement is met. In such cases, an alternate Agency credential may be issued as appropriate based on a risk determination. Before an alternate Agency credential may be issued, the Center Protective Services Office will require completion and a minimum annual revalidation of the NCHC, FBI Investigations File, Visual Compliance, and SAVE checks prior to issuance of an alternate Agency credential.

4.5.6.3 Three years residing in the U.S. is defined as any presence in the U.S. or a U.S. territory for three continuous years or more during which any absences can be regarded as temporary and do not destroy the degree of continuity necessary to establish and maintain residence. Decisions about whether a person maintains residency are based on the circumstances of the particular case and at the discretion of the CCS/CCPS.

4.5.7 The results of the check against SAVE and the Visual Compliance check shall be attached to the identity record of the foreign national in IdMAX.

4.6 Requirements for Visas

4.6.1 For the purposes of granting access to NASA, the purpose specified by the visa shall match the purpose of the visit to NASA.

4.6.2 Any visit purpose outside that specified by the visa shall be denied.

4.6.3 Visa waivers shall only be accepted in compliance with Department of State guidelines for use of a visa waiver; specifically:

a. The duration of the visit must be 90 days or less.

b. The purpose of the visit must be an activity permitted on a Visitor (B) Visa.

4.6.3.1 When a foreign national with a visa waiver needs to stay in the U.S. beyond the 90 days authorized by the visa waiver, the foreign national is required to provide the final visa information to the Center IVC who will verify the final visa information in SAVE.

4.7 Requirements Based on Type of Onsite Affiliation

4.7.1 If a foreign national is supporting NASA under an International Space Act Agreement (ISAA) and requires periodic access to NASA facilities, the foreign national shall be processed in accordance with procedures in section 4.3, On-Site Enrollment and Issuance Procedures for Foreign Nationals. An ISAA, or other agreement (e.g., contract, grant, etc.), is generally required for any short-term visit or assignment (up to 29 calendar days in a 365-day period).

4.7.2 If a foreign national is visiting NASA periodically as an accredited news media representative, the IVC shall coordinate with the Center public affairs office to obtain requisite information. Once the IVC has determined that agreement has been reached on requirements, the IVC will coordinate with the CCS/CCPS as to the level of investigation required. The foreign national will be given a physical access credential commensurate with the level of investigation performed and access requirements. Only non-PIV credentials will be issued. Investigation status information will be updated annually. Access to IT resources will be administered with a non-PIV credential.

4.7.3 If a foreign national is visiting NASA for a HLPV, the IVC shall coordinate with the Center protocol office to obtain requisite information.

4.7.4 J-1 Exchange Visitor Visa.

4.7.4.1 Under the provisions of 22 CFR Part 62, and as approved by the Department of State, NASA is authorized to conduct an exchange visitor program and can authorize foreign nationals to be assigned to NASA installations on J-1 exchange visitor visas. NASA has authority to sponsor two exchange visitor categories: Research Scholars and Government Visitors. The regulations regarding these categories and the exchange visitor program in general can be found at 22 CFR 62.1 through 62.90.

4.7.4.2 If a foreign national is visiting NASA as part of the NASA Exchange Visitor Program (J-1 Visa), the IVC shall coordinate with the sponsor to obtain requisite information and to ensure that the foreign national is part of an existing ISAA partnership.

4.7.4.3 For a foreign national to be considered for the NASA Exchange Visitor Program, the host Center or Component Facility must document its request (with appropriate justification) in a memo to the cognizant Mission Directorate or Mission Support Office at NASA Headquarters with a copy

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

to the Export Control Office and Interagency Liaison Division, OIIR, and, in parallel, contact the IVC to enter the request for review. If the Headquarters Office endorses the request, OIIR will review for final approval. If approved in principle, OIIR will prepare an ISAA between NASA Headquarters and the foreign sponsoring entity (e.g., foreign space agency or foreign university) and, once executed, if all requirements associated with authorizing a J-1 Visa have been satisfied, the authorization will be issued, covering the period of the approved assignment.

4.7.4.4 No NASA funding is provided to the foreign national under the NASA Exchange Visitor Program. All funding must come from the foreign sponsor or from personal funds, and NASA must assess if the funds available are sufficient to sustain the individual for the period of the assignment. NASA provides office space and supplies and, if necessary and approved pursuant to NASA policies, computer and network access. The period of assignment for approved foreign national participants is generally from six months to three years. Foreign nationals from designated countries and all foreign national undergraduate students are ineligible for participation in the NASA Exchange Visitor Program.

4.8 Requirements Based on Visitor Attributes

4.8.1 Dual Citizenship.

4.8.1.1 If the foreign national has dual citizenship with the U.S. and a foreign country (including designated countries), identity vetting shall follow the processes for a U.S. citizen. Any physical access restrictions will be determined and agreed to by the CCS/CCPS and the sponsor/host.

4.8.1.2 If the foreign national has dual citizenship for two foreign countries and one or both of those countries is a designated country, the identity shall be vetted as a foreign national from a designated country.

4.8.2 Foreign nationals born in a designated country shall be identity vetted and credentialed as a foreign national from a designated country. Foreign nationals from countries designated by the Secretary of State as sponsors of terrorism are generally not eligible for access to NASA facilities pending review by OIIR and in accordance with the requirements of section 4.2.4.

4.8.3 U.S. citizens employed by a foreign entity shall be treated as U.S. citizens for the purpose of identity vetting.

4.8.4 U.S. persons, Lawful Permanent Residents (LPR) and protected individuals shall be treated as U.S. citizens for the purposes of identity vetting, granting of access, and escort requirements with the following exceptions:

4.8.4.1 During identity vetting, LPRs shall be required to present a valid Permanent Resident Card (PRC) or Alien Registration Receipt Card (ARRC) (Form I-551), commonly known as a Green Card, to verify and establish LPR status. The Green Card shall be verified through a SAVE check or other electronic verification.

4.8.4.2 LPRs shall be issued badges that identify them as an LPR. LPR credentials will not be issued in excess of the earlier expiration date of the PRC, ARRC, or employment authorization document.

4.9 Requirements Based on Credential Type

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

4.9.1 The expiration date of credentials issued to foreign nationals shall be set for a period not to exceed the earlier of three years from the Card Production Request (CPR) generation date, agreement end date, assignment end date, visa admitted-until date, or date of I-94/W expiration.

4.10 Requirements for Remote-Only Access

4.10.1 Foreign nationals residing in the U.S. and requesting remote-only access shall be processed in accordance with the requirements in section 4.3, On-Site Enrollment and Issuance Procedures for Foreign Nationals.

4.10.2 Foreign nationals performing work for NASA while residing outside the U.S. and requesting remote-only access to very low-risk systems which do not require identity proofing shall undergo a check through Visual Compliance. Fingerprints are not required of these foreign nationals. A Visual Compliance check, by itself, is not sufficient to be granted access to low-risk, moderate-risk, or high-risk systems.

4.10.3 Foreign nationals performing work for NASA while residing outside the U.S. and requesting remote-only access to low-risk, moderate-risk, or high-risk systems shall be processed in accordance with section 4.3, On-Site Enrollment and Issuance Procedures for Foreign Nationals. Fingerprints are required of these foreign nationals.

4.10.4 Foreign nationals with remote-only access shall be given access credentials commensurate with the level of investigation performed and the access requirements.

4.10.5 Foreign national "limited privileged" access to IT systems shall be allowed only if the foreign national is involved in a program under an ISAA and the foreign national's ACP includes that access. The sponsor will verify that an ISAA and ACP are in place and has accountability for ensuring the security of IT system data being accessed by the foreign national.

4.10.6 Any foreign national having access to NASA data shall provide a written certification that they fully understand and will adhere to NASA rules and regulations regarding the integrity and confidentiality of NASA data being accessed. This certification may be a completed NASA IT Security Training or a signed document signaling understanding of IT access requirements as outlined in NPR 2810.1. Either of these activities will satisfy the completion of the NASA IT Security Training requirement prior to the activation of IT access. Recertification will be performed annually as outlined in NPR 2810.1.

Chapter 5. Characteristics of NASA Badges

5.1 NASA Credential Types

5.1.1 NASA PIV Credentials - The information on a NASA PIV credential exists in both visual printed and electronic forms. The NASA PIV credential shall be equipped with technologies that allow for physical access through a proximity antennae and logical access through an embedded chip.

a. NASA PIV credentials contain the following security and distinguishable features on the front of the card:

(1) Holographic overlay.

(2) Smart chip.

b. NASA PIV credentials have the following printed vertically on the front of the badge.

(1) The photograph of the applicant in the top left corner.

(2) The legal name of the applicant, printed below the applicant photograph.

(3) Two badge expiration dates, one located in the upper right corner (MM YYYY format) and the second to the right of the applicant photograph, below the Agency identifier and over the Agency logo (YYYYMMDD format).

(4) The NASA Agency identifier logo.

(5) The affiliation of the applicant, to the right of the applicant photograph and over the Agency logo.

(6) The NASA Agency identifier, to the right of the applicant photograph, below the affiliation, and over the Agency logo.

(7) The unique badge identification number, below the NASA Agency identifier and the affiliation color band.

(8) Solid color band across the middle of the badge, over the full name with the color determined by the affiliation of the badge holder, per section 5.1.5, Visual Color Coding for Employee Type.

c. NASA PIV credentials have the following printed horizontally on the back of the badge:

(1) Return address.

(2) Applicant height.

(3) Applicant eye color.

(4) Applicant hair color.

(5) Bar code.

5.1.2 NASA Temporary Badge - Temporary badges may be equipped with technologies that allow

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

for physical access through a proximity antennae and/or logical access through an embedded chip. Temporary badges shall not resemble the NASA PIV credential.

a. Temporary badges will have the following printed vertically on the badge:

(1) The silhouette of a vertical Space Shuttle on the right side of the badge, located above the solid affiliation color area.

(2) The photograph of the applicant in the top left corner.

(3) The legal name of the applicant, printed below the applicant photograph.

(4) The NASA Agency identifier, to the right of the applicant photograph.

(5) The designation of the issuing Center, below the applicant name.

(6) The unique badge identification number, below the NASA Agency identifier.

(7) The badge expiration date that is 180 calendar days or less from the date of Center/facility affiliation, below the badge identification number.

(8) Solid colored lower section based on the affiliation of the badge holder, per section 5.1.5, Visual Color Coding for Employee Type.

(9) OPS mailing information on the bottom front of the badge.

b. Temporary badges have the following printed horizontally on the back of the card:

(1) Return address.

(2) Applicant height.

(3) Applicant eye color.

(4) Applicant hair color.

5.1.3 NASA Visitor Badges - Centers may prescribe the topology for visitor badges as long as they meet the following criteria:

a. The legal name of the applicant.

b. The full name of the issuing Center.

c. The full badge expiration date that is 29 days or less from the date of Center/facility affiliation.

5.1.4 NASA alternate Agency credentials — Alternate Agency credentials will contain the following information:

a. The photograph of the applicant.

b. The legal name of the applicant.

c. The name of the issuing Center (Center name may be common abbreviation, e.g., ARC, DFRC, etc., as appropriate).

5.1.5 Visual Color Coding for Employee Type - NASA PIV and alternate Agency credentials use colored markings on the badge to determine the affiliation of the badge holder. NASA PIV credentials use a color band through the name of the applicant, and alternate Agency credentials use a colored lower section below the photograph and including the name. Unless otherwise indicated, the color being used is for both NASA PIV and alternate Agency credentials, as described in Table 5.1.5.

Table 5.1.5, PIV Credential Color Coding

Employee Type	Color Coding
Federal Employee	A plain white color band.
Contractor Employee	Contractors will have a green color band. On the right side of the band is a "G" inside a white circle to assist individuals with visual impairment in recognizing the green color.
Contractors at the NASA JPL	Contractors at the NASA JPL who are U.S. citizens will be recognized by the addition of a solid silver color below the green contractor color band.
Interagency Personnel Agreement (IPA) Employee	A plain white color band. The lower right corner on the front of the badge the label "IPA" will appear in black letters.
Foreign Nationals	Foreign national badge characteristics take precedence over all other affiliation characteristics. Foreign national badges have a light blue color band. On the right side of the band is a "B" inside a white circle to assist individuals with visual impairment in recognizing the light blue color. Foreign national badges have a light blue color border around the applicant photo.
Escorted Foreign Nationals	In addition to the color coding for foreign nationals as described above, foreign nationals requiring escort will be recognized by red lettered "ESCORT ONLY" across the middle of the badge.
International Partners	International partners will have a flag of the applicant's country of citizenship in the lower right corner of the badge in addition to the light blue foreign national color band and border.
Emergency Response Officials	Emergency response officials (ERO) will be recognized by a red stripe containing the words "Emergency Response Official" on the bottom of the badge in Zone 12 per the requirements of NIST Special Publication 800-104. The back of an ERO badge contains text stating their position as ERO and access permissions after verification of the badge holder's identity.

5.1.6 Emergency Response Officials (ERO) Badges - Emergency Response Office badges shall be issued only to the following persons:

a. EROs to include individuals who are:

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

(1) Continuity of Operations (COOP) and Continuity of Governance (COG) personnel associated with COOP at a NASA Center or an alternate operating site during emergency/crisis situations. This includes only those persons who are members of the Emergency Relocation Group (ERG) and their respective support staff and Emergency Operation Center (EOC) personnel who are appropriately certified and trained.

(2) Disaster response personnel for each facility who possess National Incident Management System (NIMS) training or professional certifications.

b. Personnel to be deployed to support the NASA National Response Framework (NRF) Emergency Support Function (ESF) Annexes. Support personnel may not be issued the ERO PIV credential unless they possess the above mentioned NIMS training or professional certifications.

c. NASA, special agents, NASA, security police, or security officers who have graduated from NASA Federal Law Enforcement Training and members of the NASA Inspector General (IG) staff who are sworn law enforcement officers.

d. Center protective services and security staff who provide support or other security functions for 34 emergency/contingency operations as deemed necessary by the CCS/CCPS so long as they possess the above mentioned NIMS training or professional certifications.

e. Center Directors, Deputy Center Directors, and Directors of Center Operations and their deputies.

5.1.7 Personnel who will be fulfilling support duties shall be issued a NASA PIV credential, without the ERO designation, to facilitate verification of identity and ease movement through the various checkpoints. Support personnel may not be issued the ERO PIV credential unless they possess the above mentioned NIMS training or professional certifications.

5.1.8 Table 5.1.8 details the color coding for alternate Agency credentials:

Table 5.1.8, Color Coding for Badges

Employee Type	Color Coding
Contractor	Non-PIV contractors will be recognized by a blue lower section. Non-PIV contractors at JPL who are U.S. citizens will be recognized by a silver lower section with red lettering for the "JPL" Center designation on their alternate Agency credential.
Foreign Nationals	Non-PIV foreign nationals will be recognized by a blue lower section designation on their alternate Agency credential.
Detailees	Non-PIV Detailees will be recognized by a white lower section designation on their alternate Agency credential.
Interns and Grantees	Interns and grantees will be recognized by an alternate Agency credential with a white lower section designation on their alternate Agency credential.
Escorted Foreign Nationals	In addition to the color coding for foreign nationals as described above, foreign nationals requiring escort will be recognized by red lettered "ESCORT ONLY" across the middle of the badge.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

5.1.9 Badges for Press Corps - The press corps shall be recognized by the word "PRESS" printed vertically down the right side of the alternate Agency credential. U.S. press corps will be further recognized by a brown lower section. Foreign national press will also contain all characteristics from the foreign national color coding as detailed in Table 5.1.5.

5.2 NASA PIV Credential Data

5.2.1 Data printed on a NASA PIV credential shall consist of:

a. Name (last name, first name, and middle initial).

b. Photo.

c. Affiliation (civil servant, detailees, contractor, grantee, or foreign national, etc.).

d. Badge expiration date.

e. Badge number consisting of a three-digit Center code plus six unique digits and printed as a number on the front, and a 3x9 bar code on the back.

f. Height, eye color, and hair color.

g. Agency card serial number, preprinted and used for tracking card stock.

h. Issuer identification consisting of a six character department code, the Agency code for NASA, and a five-digit issuing facility number.

5.2.2 The digital data stored on the NASA PIV credential supports physical and/or logical access use, encryption, and signing capability and provides security and authentication protection for the PIV credential and PIV credential holder.

5.2.2.1 Card Holder Unique Identifier (CHUID) - The CHUID is used by access control applications and is the only data that is accessible through both the contact and contactless interfaces. Applications can read this data without any action from the badge holder. The CHUID is composed of:

a. Federal Agency Smart Credential Number (FASC-N).

b. NASA Agency code.

c. System code identifying the original issuing Center.

d. A credential number.

e. PIV credential holder's Uniform Universal Personal Identification Code (UUPIC).

f. Expiration date.

5.2.2.2 Digital Certificates

a. PKI X.509 certificates are used for authentication of the PIV credential and digital signing, encryption, and authentication of the PIV credential holder.

b. Credentials used for logical access have a certificate for PIV credential authentication. Additional

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

certificates are loaded based on the duties and needs of the PIV credential holder.

5.2.2.3 Biometrics (typically fingerprints of the right and left index fingers) are stored as minutiae templates that represent a specific biometric, but cannot be reverse-engineered to recreate an image of that biometric.

5.2.2.4 Digital Representation of Printed Information - Certain items printed on the front and back of the card are stored on the chip as a security and authentication measure; including name, affiliation, organization, badge expiration date, Agency card serial number, and issuer identification.

5.2.2.5 Photograph - The facial image used in creating the photo printed on the front of the badge is stored in the badge. A facial image is required, and obscuring headwear may not be worn for the photograph.

5.2.2.6 The PIN is used to secure and protect the electronic data stored on the PIV credential. The PIN is used by the PIV credential holder to allow applications to access data and as part of the authentication process. It is stored in a secure section of the smart card, separate from the rest of the PIV credential digital data. All PIV credential data, with the exception of the CHUID, require the PIV credential holder to enter their PIN before an application can either access or use the data. The PIN is a minimum of a six-digit number selected by the PIV credential holder and written to the PIV credential during finalization. It is not stored in the identity management system and should not be written down or otherwise recorded by the PIV credential holder. The PIV credential is automatically locked after no more than 15 consecutive tries of entering an invalid PIN. PIV credential PIN reset details and requirements for resetting a PIN are identified in Section 6.7.

5.3 The Uniform Universal Personal Identification Code (UUPIC)

5.3.1 UUPIC System Management - The UUPIC system is the database and application that stores personnel information required for the creation of unique identities and that generates the UUPIC. This system shall be owned by OPS, working in concert with the OCIO and OCHCO, to ensure proper functioning, assignment, use, and protection of the UUPIC system. OPS is responsible for administrative identity management in the UUPIC system. The UUPIC system will be treated as a high confidentiality, integrity, and reliability system. Access to the system will be controlled by two-factor authentication, firewalls, and encryption techniques. The UUPIC generated by the system may be available to NASA employees for lookup and may be used for positive identification of individuals within NASA information systems. However, the UUPIC may not be used as a login identifier or user account name for any information systems, databases, Web sites, etc. Additionally the UUPIC may not be used for purposes other than those described above without the concurrence of the AIMO and the Director of Agency Workforce Systems, within OCHCO (or assigned delegate), with the exception of account initiation in the identity management system. System owners requiring access to the UUPIC system will submit a signed Service Level Agreement (SLA) and/or Memorandum of Understanding (MOU) to OPS.

5.3.2 Approval to Access the UUPIC System - The system owner requiring access to the UUPIC system shall submit a signed SLA/MOU to the ICAM Logical Access Management team detailing the purpose for accessing the UUPIC system. The ICAM Logical Access Management team will work with the system owner to ensure proper documentation and authority to access the UUPIC system. The ICAM Logical Access Management team will make a recommendation to approve or

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

disapprove UUPIC system access to the AIMO. In the event of a denial for UUPIC access, the requesting system owner may appeal by sending a letter, along with the SLA/MOU, to OPS and OCIO. OPS and OCIO will respond with a final decision within 60 days of receipt of the appeal.

5.3.3 UUPIC Characteristics - UUPICs shall only be issued through the population of seed data (name, SSN or foreign national visitor number for foreign nationals without a SSN, and date of birth) into the UUPIC database. This information is required for all NASA civilians, contractors, partners, and remote IT system users. Any request for an UUPIC will be initiated via an approved work-flow method. The UUPIC database will auto-populate the NIMS, Identity Management System (IDMS), and EPACS upon returning a UUPIC number. The reliable assignment of the UUPIC to persons uses at least two unique attributes, in addition to name attributes, from approved identity source documents. The Agency directory is used as the UUPIC repository for general access to the UUPIC number. UUPIC numbers will be issued in random sequence, consistent with NASA policy, and will meet the following requirements:

a. Is a nine-digit numerical code without any significance as to the characteristics of the individual.

b. Is displayed as a set of 3 x 3 x 3 numbers, for example: 123 456 789.

c. Cannot be reverse-engineered based on other data contained in the UUPIC application.

5.3.4 UUPIC Usage - The UUPIC shall serve as a replacement for the SSN by providing a unique identifier that can serve as a data point across NASA information systems. Therefore, the UUPIC may not be used as a login identifier or user account name for any information systems, databases, Web site, etc. With the exception of account initiation in NIMS, use of the UUPIC for any identification purposes outside those needed for positive identification of individuals across and only within information systems is prohibited without the consent of the AIMO. The UUPIC may never be posted on any Internet accessible Web site. Any deviation from this policy will be coordinated with OPS through OCIO in advance. Requests for an UUPIC will be initiated via the approved workflow method. The UUPIC database will auto-populate the appropriate identity management systems upon returning a UUPIC number. UUPIC numbers are stored internally along with the first, middle, and last names and other information necessary to uniquely associate the UUPIC with a person.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

Chapter 6. PIV Credential Management Lifecycle

6.1 PIV Credential Inventory

6.1.1 Ownership. A PIV credential is not personal property, but is the property of the U.S. Government. All personnel shall be responsible for appropriately safeguarding issued credentials, immediately reporting the loss or false use of a PIV credential, challenging noncredentialed personnel, notifying the proper authority of a name change, properly displaying a PIV credential when on NASA property, and surrendering a PIV credential upon resignation, retirement, or the direction of the issuing authority.

6.1.2 Reciprocity. PIV credentials issued by other Federal Government departments and agencies shall be accepted for the purpose of establishing the identity of the individual.

6.1.3 Misuse. Forging, falsifying, or allowing misuse of a PIV credential or other forms of NASA identification in order to gain unauthorized access to NASA physical and logical resources is punishable under 18 U.S.C. 799 by fine or imprisonment for not more than one year, or both, and may further result in termination of employment and access to NASA resources.

6.1.4 Production. Printing of credentials shall only be performed by approved personalization service providers and will be shipped directly to a Center by the service provider.

6.1.5 Stock protection. Unprinted or unfinalized PIV credentials shall be shipped directly to a Center by the PIV credential manufacturer. The PIV credential issuing facility manager or other appropriate authority will designate a point of contact that is responsible for receipt of, signing for, and inventory and storage of PIV credential stock. PIV credential stock will be accessible only by authorized personnel and maintained in a secure manner, pursuant to Section 6.2, PIV Credential Storage and Handling. PIV credential stock will be monitored through the use of a log which includes, at a minimum, the date of check in, the date of check out, and the name of the person(s) performing the PIV credential stock check-ins or check-outs.

6.2 PIV Credential Storage and Handling

6.2.1 Credentials shall be stored using the following minimum requirements:

a. Properly identified and treated as "controlled material" for inventory.

b. Segregated from classified materials, firearms, ammunition, or currency.

c. Stored in a secure area protected by guard(s), key lock(s), and/or card reader(s).

6.2.2 Credentials which are lost, stolen, or unaccounted for while in storage shall be reported immediately or within 24 hours to the PIV credential issuing facility manager after discovery. PIV credential details, including PIV credential identification numbers and status, will be reported to the NEACC within 24 hours of discovery in order to update the card management system. The PIV credential issuing facility manager will forward a report outlining all pertinent facts to the OPS

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

Security Management Division Director no later than two days after receiving reports of the lost, stolen, or unaccounted for credentials.

6.2.3 A defective PIV credential shall be identified, reported, and delivered to the core technical team. The issuance official will record the defective PIV credential identification number and the defective status in the PIV credential storage log. A new PIV credential will be created following Sections 3.4.4 of this document.

6.2.4 All PIV credential encoding failures shall be reported to the core technical team within five days of discovery and include the identification number, failure description, and any other pertinent information.

6.2.4.1 PIV credential encoding failures include:

a. Rejection by a card reader or machine.

b. Error message(s) during encoding of the PIV credentials.

c. PIV credential is not recognized by physical access control systems (PACS) or logical access control systems (LACS).

6.2.4.2 If the PIV credential becomes defective as a result of the encoding failure, refer to Section 6.2.3 of this NPR.

6.3 Final Adjudication and Subsequent Investigation

6.3.1 Final adjudication may occur at any time in the process. Final adjudication should be conducted within 90 days of receipt of the background investigation. Final adjudication may occur after the issuance process has completed and an applicant has received a PIV credential following favorable fingerprint check results. Upon receipt of the background investigation, the authorizer shall adjudicate the results of the background investigation as favorable or unfavorable. This adjudication will be documented and performed in accordance with OPM policy.

6.3.2 When background investigation results are favorable, the authorizer shall update the applicant's record to reflect favorable adjudication of the background investigation and the background investigation indicator in the PIV credential data model will be set to indicate background investigation completion. When background investigation results are unfavorable, the authorizer will update the applicant's record to reflect unfavorable determination of the background investigation result. The authorizer will revoke all physical and logical access rights associated with the PIV credential. The PIV credential will be immediately confiscated. The sponsor will be notified of the denial decision.

6.3.3 The PIV credential holder shall be provided the opportunity to appeal, pursuant to NPR 1600.3. If the PIV credential holder does not appeal or if the appeal is denied, the identity associated with the confiscated PIV credential will be terminated and the credential will be destroyed.

6.4 Credential Usage: Display, Protection, and Proper Usage

6.4.1 NASA shall provide an electromagnetically opaque badge holder selected from an approved products list to physically protect the badge and electronically protect the information contained in the badge. Other holders found on the approved products list may be purchased by a Center at their discretion. Such holders are the responsibility of the purchasing Center to ensure that they are electromagnetically opaque. The badge will be properly displayed and worn at all times while the bearer is on a NASA Center or component facility. They will be worn above the waist on the outermost garment with the photograph visible. The use of a permanent-type symbol or the affixing of any device (e.g., tenure pin, decals, etc.) on a PIV credential (or any alteration or modification thereof) is not allowed.

6.4.2 PIV credentials held by both civil servants and contractors shall be accepted at all Centers for access to public areas and authorized IT resources at that Center. Access to non-public areas at each Center will be handled on an as-needed basis in compliance with the policies established by that Center for access to facilities and/or IT resources. Silver JPL contractor PIV credentials will be accepted at all NASA Centers.

6.4.3 NASA alternate Agency credentials and visitor badges shall only be used for access to the Center or facility from which it was issued. NASA alternate agency credentials and visitor badges may be used for access to secure NASA computer systems and networks. Policies for temporary access to NASA IT resources are addressed by NPR 2810.1.

6.4.4 The visitor badge shall only be valid for the term issued, pursuant to section 3.3.4, NASA Visitor Badges. The visitor badge will be returned at the end of the visit. Individuals who are issued an escort-required visitor badge will be escorted by an individual holding a valid NASA PIV credential.

6.4.5 A CCS/CCPS may authorize issuance of alternate Agency credentials for the following purposes:

a. To provide access for relatives, guardians, or next of kin to wellness facilities (child care, healthcare, etc.).

b. To provide visual verification in the absence of electronic verification for PIV credentials issued by another Federal agency and department.

c. To recognize retirees and other individuals previously affiliated with NASA (such as ex-astronauts) who no longer require access for official NASA business.

6.4.6 PIV credential usage requirements related to logical access are established in the NASA Subscriber Agreement, provided to and signed by the applicant for:

a. Authorized uses of the PIV credential.

b. Authorized uses of the PKI certificates and services provided with the PIV credential.

c. Additional usage requirements for logical access credentials are established in NPR 2810.1, Security of Information Technology.

6.4.7 The background investigations associated with the issuance of the CAC by DoD have been determined by OPM to be equivalent to the background investigation requirements for issuing a PIV credential. Centers will continue to issue a NASA alternate Agency credential that reflects the individual's authorization to access the Center. This differentiates the DoD employee working at a Center from the one at home on leave. PIV credentials issued by other Federal Government agencies will be accepted for the purpose of identity verification at a Center. Access will be granted to the facility using a NASA alternate Agency credentials or the PIV credential with a card reader to establish granted access rights.

6.5 PIV Credential Renewal

6.5.1 Credential renewal shall occur prior to PIV credential expiration and facilitate replacement of the PIV credential without the need to repeat the full enrollment and reissuance procedures described in Section 3.5. PIV credential holders may apply for a renewal starting six weeks prior to the expiration date on their PIV credential. The PIV credential holder will coordinate with the sponsor, who ensures personnel records are accurate and current before the issuance of a new PIV credential. New biometrics are collected as described in Section 3.5.4. The old and/or expired PIV credential is to be collected and destroyed at the time of renewal pursuant to Section 6.14, PIV Credential Destruction. If warranted, the authorizer will approve the renewal and coordinate the request for a new background investigation to be performed. If a renewal is in process and is not completed before the enrollment is completed, then the credential must be re-issued as described in Section 6.6.

6.6 PIV Credential Re-issuance

6.6.1 The old PIV credential shall be revoked, pursuant to Section 6.8, PIV Credential Revocation for the following conditions, and the applicant will undergo the entire registration and issuance process. PIV credential re-issuance will occur when the PIV credential:

a. Has reached its expiration date.

b. Has been compromised.

c. Is lost, stolen, or damaged.

d. Requires a change in printed information (name change, citizenship change, etc.) or card holder's status.

6.6.2 NASA PIV credentials shall not be re-issued for an individual transferring from one Center to another Center.

6.6.3 PIV credential holders who have officially changed their name shall submit a request for a reissuance of their PIV credential. The PIV credential holder will be required to reenroll and provide approved identity source documentation that reflects the legal name change prior to enrollment occurring and issuance of the new PIV credential.

6.7 PIV Credential PIN Reset

6.7.1 Credentials that are disabled or locked-out due to a maximum of 15 consecutive invalid PIN entry attempts shall have their PIN reset. It is the responsibility of the PIV credential holder to arrange for a PIN reset to occur. Biometric verification of the applicant's biometrics to the biometrics stored on the card will occur prior to the PIV credential being returned to the applicant. PIN reset does not require the reissuance of a PIV credential.

6.8 PIV Credential Revocation

6.8.1 Credentials shall be revoked under the following conditions:

a. Exit on duty.

b. Change in need for access.

c. Termination of employment.

d. Unfavorable fingerprint check or background investigation determinations.

e. Death of the PIV credential holder.

6.8.2 Revocation of a PIV credential shall result in the following:

a. The PIV credential holder's relationship shall be set to "inactive."

b. The PIV credential shall be returned and terminated.

c. Notification shall be provided to the sponsor of the PIV credential revocation.

6.9 Lost and Stolen Credentials

6.9.1 Lost and stolen credentials shall be reported to the PIV credential Issuing Facility Manager within 18 hours of discovery of the loss/theft. The PIV credential holder will, within five business days of reporting the loss/theft, appear in person at the badging office and provide their SSN or Foreign National Management System Identification Number (FNMSID) to verify loss/theft of the PIV credential and be issued a new PIV credential. The lost/stolen PIV credential will be revoked and/or disabled, cancelling all certificates and access privileges of that card. The identity of the PIV credential holder itself will remain active, as only the card is disabled. The PIV credential holder will be required to undergo a PIV credential re-issuance per Section 6.6 PIV Credential Re-issuance. Until the new PIV credential is created, the PIV credential holder will obtain a visitor or alternate Agency credential (non-PIV) and temporary non-PIV logical assess credentials per NPR 2810.1, Security of Information.

6.9.2 It is the responsibility of NASA Centers to establish policy for the handling of multiple lost and stolen credentials. Centers may adopt one of the below methods for managing PIV credential holders who report their PIV credential as lost or stolen on multiple occasions. The following list is not comprehensive, and additional methods may be chosen by the Center:

a. Allow for the replacement of two credentials after which the PIV credential holder will undergo awareness training for each subsequent lost PIV credential prior to receiving the PIV credential.

b. Implement a lost/stolen PIV credential form which requires signature of the PIV credential holder's manager, sponsor, or other appropriate individual(s).

6.10 Forgotten Credentials

6.10.1 It is the responsibility of NASA Centers to establish policy for the handling of forgotten credentials. Centers may adopt any number of the below methods for managing PIV credential holders who forget their PIV credential. The following list is not comprehensive and additional

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

methods may be chosen by the Center:

a. Require the PIV credential holder to retrieve the PIV credential.

b. Allow issuance of a visitor badge to the PIV credential holder with verification of identity through approved identity source documents such as a driver's license.

c. Suspend the forgotten PIV credential until the PIV credential holder appears in the badging office with the forgotten PIV credential for it to be activated.

6.11 PIV Credential Suspension

6.11.1 Credentials shall be set to "suspended" and temporarily disabled when the

PIV credential has been misplaced and the PIV credential holder knows the current location of the PIV credential but cannot retrieve it at this time. Lost or stolen credentials will be handled pursuant to Section 6.9, Lost and Stolen Credentials. The PIV credential holder will appear at the badging office, no later than 18 hours after discovery of the misplacement, and file a report stating the PIV credential has been misplaced and provide the location of the PIV credential that was last known. Until the PIV credential is recovered or declared lost or stolen, the PIV credential holder will obtain a visitor or alternate Agency credential. PIV credential holders will report to the badging office within five business days of the original report to update the PIV credential status as being recovered, lost, or stolen. Lost and stolen credentials will adhere to Section 6.9, Lost and Stolen Credentials. Credentials that are found will be set to "active" upon report of the PIV credential being found and visual confirmation of the PIV credential. Any alternate Agency credential or visitor badge that was issued will be returned.

6.12 PIV Credential Return

6.12.1 Credentials shall be returned to NASA once an individual's affiliation with NASA has ended. Credentials should be returned to the issuing authority no later than the last day of association with NASA. The issuing authority will be responsible for recording receipt of the PIV credentials that are returned and properly storing the PIV credentials until destruction. Credentials are not allowed to be kept as souvenirs. The responsibility of PIV credential return oversight will be:

a. HR for NASA civil servant.

b. Contract program manager for contractors.

c. Grant technical official for grantees.

d. IVC for foreign nationals.

6.13 PIV Credential Termination

6.13.1 Credentials returned to the badging office that do not meet any of the requirements previously established in this chapter and are to be terminated shall have all data, certificates, and access privileges invalidated, revoked, and/or disabled. Credentials that are to be terminated will have their status set to "terminated," and a reason will be supplied for the termination. Deactivation of a PIV credential and associated identity will be completed within 18 hours of notification of the need for

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

PIV credential termination. Terminated credentials will be destroyed following the requirements in Section 6.14, PIV Credential Destruction.

6.14 PIV Credential Destruction

6.14.1 Credentials meeting the following criteria shall be destroyed:

a. Expired credentials.

b. Credentials discovered or located after being declared lost or stolen.

c. Credentials that are damaged.

d. Terminated credentials.

6.14.2 Credentials shall be thoroughly destroyed using heavy-duty cross cut shredders that are capable of smart card destruction, by depositing into a burn bag for burning, or by more rigorous methods.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

Appendix A: Definitions

Access – With regard to NASA assets, the explicit granting of permission to enter and/or use NASA facilities, interact with NASA personnel, and/or use NASA information and related information processing services.

Access Control – The process of granting or denying specific access requests.

Access Control Plan (ACP) – For a program, project, or foreign national, the assets to which that foreign national may request access. For additional information, refer to NPR 2190.1, NASA Export Control Program. Formerly known as a Technology Transfer Control Plan (TTCP)/Security Technology Transfer Control Plan (STTCP).

Accreditation – Formal declaration by a Designated Approving Authority (DAA) that an IT system is approved to operate in a particular security mode for the purpose of processing CNSI, using a prescribed set of safeguards. Accreditation Authority is synonymous with DAA.

Adjudication – A fair and logical Agency determination, based upon established adjudicative guidelines and sufficient investigative information, as to whether or not an individual's access to classified information, suitability for employment with the U.S. Government, or access to NASA facilities, information, or IT resources is in the best interest of national security or efficiency of the Government.

Alternate Agency Credential – Non-PIV credentials which have been approved by the AIMO as standard templates across the Agency and may allow physical and/or logical access to NASA facilities and systems. Formerly known as a Center-specific badges.

Asset – A system, object, person, or any combination thereof that has importance or value; includes contracts, facilities, property, records, unobligated or unexpended balances of appropriations, and other funds or resources.

Authentication – (1) The validation and confirmation of a person's claim of identity. (2) The validation and identification of a computer network node, transmission, or message. (3) The process of establishing confidence of authenticity. (4) Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to facilities and information systems.

Authorization – The privilege granted to a subject (e.g., individual, program, or process) by a designated official to do something, such as access information based on the individual's need to know.

Background Investigation – The process of looking up and compiling criminal records, commercial records, and financial records of an individual.

Badge – See definition for Credential. A physical credential with visual elements that enable an authorized person (e.g., security officer) to grant access using a NASA-approved authentication mechanism.

Center Chief of Protective Services (CCPS) – See definition for Center Chief of Security (CCS).

Center Chief of Security (CCS) – The senior Center security official who is responsible for management of the Center security program.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

Certification – A formal process used by the certifying official to ensure that an individual has met all established training requirements as necessary to perform their security responsibilities.

Component Facilities – NASA-owned facilities not located on any NASA Center (e.g., Michoud Assembly Facility, Wallops Flight Facility, White Sands Test Facility, and NASA IV&V).

Contractor – For the purpose of this NPR, any non-NASA entity or individual working on a NASA installation or accessing NASA IT for an employer who is subject to Executive Order 11246.

Credential – A physical/tangible or electronic object through which data elements associated with an individual are bound to the individual's identity. Credentials utilize NASA-approved authentication mechanisms to grant physical and/or logical access to assets.

Designated Country – A country with which the United States has no diplomatic relations, a country determined by the Department of State to support terrorism, a country under Sanction or Embargo by the United States, and/or a country of Missile Technology Concern. A current list of NASA designated countries can be found in IdMAX or on the OIIR webpage at https://oiir.hq.nasa.gov/nasaecp.

Escort – The management of a visitor's movements and/or accesses through the constant presence and monitoring of the visitor. Escorts are trained and designated holders of a NASA PIV, DoD CAC, or other Federal agency PIV that has been registered in IdMAX.

Exception – The approved continuance of a condition authorized by the AA for OPS that varies from a requirement and implements risk management on the designated vulnerability.

Foreign National – Any person who is not a U.S. citizen or U.S. person (lawful permanent resident or protected individual).

Foreign National from a Designated Country – Any foreign national born in or with a citizenship from one or more designated countries.

Grant Recipient – Organization (i.e., universities, nonprofits, etc.) that has received a Federal award (grant or cooperative agreement) directly from NASA to carry out an activity under a NASA program.

High-Level Protocol Visit (HLPV) – Any visit by individuals representing or delegations of foreign heads of state or government, ambassadors or heads of foreign government ministries, or space agencies.

Identity – The set of attributes that uniquely identify an individual for the purpose of gaining logical and physical access to protected resources and identification in electronic transactions.

Identity Proofing – The process for providing sufficient information (e.g., identity history, credentials, and documents) to a Registration Authority (RA) when attempting to establish an identity or issue a credential.

Identity Source Document – A NASA-approved document used to verify aspects of a person's identity. The list of NASA-approved identity source documents can be found in the ICAM Portal.

Identity Verification – The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the credential or system and

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

associated with the identity being claimed.

Identity Vetting – A review of information about a person for possible approval or acceptance. In this document, a vetted person has been reviewed to determine eligibility for access to NASA physical and/or logical assets.

International Partners – Foreign entities or persons who are involved in a particular international program or project under an International Space Act Agreement (ISAA).

Lawful Permanent Resident (LPR) – An individual defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3). A foreign national, legally permitted to reside and work within the U.S. and issued the Permanent Resident Card (PRC) or Alien Registration Receipt Card (ARRC) (Form I-551), also known as a Green Card. LPRs may be employed in the Federal sector for specific needs or under temporary appointments per 5 CFR, Part 7, Section 7.4). LPRs may not be granted access to classified national security information (CNSI). LPRs are not prohibited from accessing export controlled commodities, but must still have a work-related "need-to-know" and are still considered foreign nationals under immigration laws. Replaces the term "Permanent Resident Alien (PRA)."

Limited privileged access – Granted to a user to use system-level commands and files to bypass security controls for part of a system.

Logical Access – Access to information records, data, and information technology systems and applications.

Long-term – Any access by a foreign national for a period of 30 calendar days or more in a 365-day period. An individual requiring long-term access is defined as temporary (30 to 179 calendar days in a 365-day period) or permanent (180 calendar days or more in a 365-day period).

National Criminal History Check (NCHC) – A background check procedure performed by the FBI Criminal Justice Information Services Division. This check returns a listing of certain information taken from fingerprint submissions retained by the FBI in connection with arrests and, in some instances, Federal employment, naturalization, or military service. If any results related to an arrest are found, the results will include the name of the agency submitting the fingerprints to the FBI, the date of the arrest, the arrest charge, and the disposition of the arrest, if known to the FBI. Commonly referred to as an identity history summary check or fingerprint check.

National Crime Information Center (NCIC) – A background check procedure performed by the FBI. This check involves a search of the records stored in the FBI Central Records System Universal Index for any appearance of the name, as well as close phonetic variants and permutations of that name. If any occurrences of the name are found, relevant paper and electronic files are retrieved from local FBI offices and from other law-enforcement agencies and analyzed. Commonly referred to as a name check, name query, or name search.

Privileged Access – Access granted to a user so that files, processes, and system commands are readable, writable, executable, and/or transferable. This allows a user to bypass security controls.

Protected Persons – A non-U.S. citizen allowed into the country under "refugee," "displaced person," and "religious or political" persecution status.

Revocation – The removal of an individual's eligibility to access physical or logical assets based upon an adjudication that continued access poses a risk to the Agency.

Risk-Based Determination – An official acknowledgement by a management official that they accept the risk posed by not implementing a recommendation or requirement, designed to reduce or mitigate the risk.

Risk Management – A means whereby NASA management implements select measures designed to reduce or mitigate known risks.

Short-term – Any visit enabling physical-only access for a period of up to but not exceeding 29 calendar days in a 365-day period. An individual requiring short-term physical-only access is defined as a visitor. These visits are generally escorted.

Smartcard – Credential issued with an individual's unique vetted identity information encoded and physically printed on the exterior and with embedded integrated circuits which can process data.

Tenant – Any individual or organization not affiliated with NASA who occupies land or property within the NASA perimeter.

Tier I Background Investigation – The minimum background investigation required for issuance of a PIV credential. This investigation includes checks of claimed identity information (date and place of birth, citizenship/status, and social security number), criminal history (law enforcement agencies), military service (conduct and discharge), educational history, employment history, Federal debt, terrorism, conduct, alcohol abuse, and drug use/involvement. For credentialing purposes, this is valid for ten years, at which point a reinvestigation must occur.

Tour – A subset of visit; a guided excursion, generally offered to the general public, by which escorted access is granted to non-public areas of interest on a Center.

Transient – A person (i.e., construction worker, club member, childcare drop off/pickup, delivery driver, retiree, Center transit, and others requested by Center Chiefs of Protective Services/Security and approved by the AIMO) who requires intermittent physical-only access for 180 calendar days or more in a 365-day period.

U.S. Citizen (U.S. National) – As defined by 8 U.S.C. Chapter 12, Subchapter III and in Parts I and II, any individual having been born in the United States or certain territories or outlying possessions of the United States and subject to the jurisdiction of the United States; born abroad to a parent or parents who were citizens at the time of birth while meeting certain other requirements; or granted citizenship after fulfilling the requirements necessary to be granted naturalization.

U.S. Person (non-U.S. Citizen) – For the purpose of implementing protection and accountability under the International Traffic in Arms Regulations (ITAR); a person who is an LPR as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3).

Visa – Issued by the Department of State, a visa indicates eligibility to seek entry to the United States for a specific purpose. Admission to the U.S. for a specified status and duration is controlled by Department of Homeland Security Customs and Border Protection inspectors.

Visa Waiver – The Visa Waiver Program (VWP) allows citizens of participating countries to travel to the United States without a visa for stays of 90 days or less, when they meet all requirements, per Department of State rules and regulations. Travelers must be eligible to use the VWP and have a valid Electronic System for Travel Authorization (ESTA) approval prior to travel.

Visit – Any means by which, and any duration for which, access is obtained to non-public NASA assets.

Visitor – Any person who needs physical-only access to a NASA facility for less than 30 calendar days in a 365-day period.

Waiver – The approved continuance of a condition authorized by the AA for OPS that varies from a requirement and implements risk management on the designated vulnerability.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

Appendix B: Acronyms

AA	Associate Administrator
ACP	Access Control Plan
AIMO	Agency Identity Management Official
ARRC	Alien Registration Receipt Card
BICE	Bureau of Immigration and Customs Enforcement
C&A	Certification and Accreditation
CA	Certification Authority
CAC	Common Access Card
CCPS	Center Chief of Protective Services
CCS	Center Chief of Security
CEA	Center Export Administrator
CHUID	Cardholder Unique Identifier
CIA	Central Intelligence Agency
CISA	Counterintelligence Special Agent
CNSI	Classified National Security Information
CPR	Card Production Request
COG	Continuity of Governance
COOP	Continuity of Operations
COR	Contracting Officer's Representative
CSCA	Commercial Space Competitiveness Act
CSLA	Commercial Space Launch Act
DAA	Designated Accreditation Authority
DCII	Defense Clearance and Investigations Index
DoD	Department of Defense
EO	Executive Order
EOC	Emergency Operations Center
EPACS	Enterprise Physical Access Control System
E-QIP	Electronic Questionnaire for Investigation Processing
ERG	Emergency Relocation Group
ERO	Emergency Response Official

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

ESF	Emergency Support Function
ESTA	Electronic System for Travel Authorization
FAR	Federal Acquisition Regulation
FASC-N	Federal Agency Smart Credential Number
FBI	Federal Bureau of Investigation
FFRDC	Federally Funded Research and Development Center
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards
FNMSID	Foreign National Management System Identification Number
GAO	Government Accountability Office
GIC	Grant Information Circular
HLPV	High-Level Protocol Visits
HR	Human Resources
HRO	Human Resources Office
HSPD	Homeland Security Presidential Directive
ICAM	Identity, Credential, and Access Management
IdMAX	Identity Management and Account Exchange
IDMS	Identity Management System
IG	Inspector General
IIF	Information in Identifiable Form
IPA	Intergovernmental Personnel Act
ISAA	International Space Act Agreement
IT	Information Technology
ITAR	International Traffic in Arms Regulations
IVC	International Visit Coordinator
JPL	Jet Propulsion Laboratory
LACS	Logical Access Control System
LPR	Lawful Permanent Resident
MOU	Memorandum of Understanding
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NAFI	Non-Appropriated Funds Instrumentality

NAMS	NASA Access Management System
NASA	National Aeronautics and Space Administration
NCHC	National Criminal History Check
NCIC	National Crime Information Center
NEACC	NASA Enterprise Applications Competency Center
NIMS	National Incident Management System
NIST	National Institutes of Standards and Technology
NM	NASA Memorandum
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
NRF	National Response Framework
OCIO	Office of the Chief Information Officer
OIIR	Office of International and Interagency Relations
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OPS	Office of Protective Services
PACS	Physical Access Control System
PCI	PIV Card Issuer
PKI	Public Key Infrastructure
PIA	Privacy Impact Assessment
PIF	PIV Issuing Facility
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PRC	Permanent Resident Card
PRD	Position Risk Determination
SAO	Senior Authorizing Official
SATERN	System for Administration, Training, and Educational Resources
SAVE	Systematic Alien Verification for Entitlements
SBU	Sensitive But Unclassified
SII	Security/Suitability Investigations Index
SLA	Service Level Agreement

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

SORN	System of Records Notice
SP	Special Publication
SSN	Social Security Number
STI	Scientific and Technical Information
U.S.	United States
U.S.C.	United States Code
USCIS	United States Citizenship and Immigration Services
UUPIC	Universal Uniform Personal Identification Code
WTTS	Workforce Transformation Tracking System

Appendix C: NASA PIV Photo Identification Badge Standards

Table C-, NASA Photo Identification Standards

1. LETTERING	COLOR-FONT	POINT
a. Badge No: ######	Black-Helvetica	6pt. Upper & lower case. Left Justified.
b. First/MI/Last Name	Black-Helvetica	12 pt. Upper & lower case. Lower left justified.
c. Center Numerical Designation	Black-Helvetica	18 pt. Lower left.
d. P.O. Box	Black-Helvetica	6 pt. Upper & lower case. Bottom centered.

2. NASA PHOTO-ID STANDARDFEATURES	CHARACTERISTIC	SIZE
a. Photograph	Color	(2.9cm x 3.9cm) 7 x 9 picas.
b. Card Stock	Standard	(5.5cm x 8.6cm) 13 x 20.3 picas.
c. Strap Slot (authorized for alternate Agency credential specific photo-ID only.	Precut & Centered	(1.4cm x .3cm) 3.5 x 7 picas.
d. Logo	Silhouette of Space Shuttle	
e. Reliability color for all Photo-ID	White	

3. COLOR CODING	CARD COLOR
a. Civil Service	WHITE
b. Consultant/Contractor/Press	GREEN
c. Military/Other Agency (Detailee)	WHITE
d. Interns/Co-Ops, Summer Students	WHITE
e. Foreign National	LIGHT BLUE
f. Jet Propulsion Laboratory	SILVER

4. CENTER	CENTER ALPHA DESIGNATOR
a. Ames Research Center	ARC
b. Armstrong Flight Research Center	AFRC

c. Glenn Research Center	GRC
d. Goddard Space Flight Center	GSFC
e. NASA Headquarters	HQ
f. Jet Propulsion Laboratory	JPL
g. Johnson Space Center	JSC
h. Kennedy Space Center	KSC
i. Langley Research Center	LARC
j. Marshall Space Flight Center	MSFC
k. Stennis Space Center	SSC

PART 2.

Privacy Act Notice

a. General - Pursuant to 5 U.S.C. 552a, Public Law 93-579, Privacy Act of 1974, as amended, the following information is being provided to persons who are asked to provide information in order to obtain a NASA Personal Identity Verification (PIV) Card.

b. Authority - This information is collected under the authority of the National Aeronautics and Space Act, 51 U.S.C. § 20132, and Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons.

c. Purposes and Uses - The primary use of collecting the information requested by this form is to facilitate the issuance of a NASA PIV Card. Social security numbers are requested to keep NASA records accurate because other employees may have the same birth date. When collected, this information shall be maintained in NASA Privacy Act Systems of Records (10SECR). Generally, the information contained in this category of records is used within NASA for determining suitability for Federal employment and access to classified information (security clearances), as well as access to security areas, NASA Centers, and other matters connected with security programs and operations.

d. In addition to the internal uses of such information, it shall also be disclosed to Federal, state, local, or foreign agencies in connection with official business, including law enforcement, intelligence activities, determinations concerning access to classified information, and matters concerning immigration. Information connected with law enforcement or administrative inquiry or investigation will be disclosed to NASA contractors, subcontractors, or grantees. Disclosure will also be made to the White House or Congressional offices in the course of certain inquiries. Additionally, in the event of a courts or formal administrative proceeding, information will be disclosed in the course of presenting evidence or during pretrial discovery. NASA will disclose information to the Department of Justice or other agencies in connection with such a proceeding.

e. Effect of Non-Disclosures - Providing this information is voluntary. However, if the form is not completed, a NASA PIV Card shall not be obtained. This may result in various undesired actions, such as disqualification for employment or access.

Appendix D: Subscriber Agreement

D.1 NASA Public Key Infrastructure (PKI) Subscriber Agreement (HSPD-12 compliant badge) (version 1.0, August 2007):

D.1.1 YOU SHALL READ THIS NASA PKI SUBSCRIBER AGREEMENT BEFORE REQUESTING, ACCEPTING, OR USING A NASA HSPD-12 COMPLIANT BADGE. BY SUBMITTING A REQUEST FOR A NASA HSPD-12 COMPLIANT BADGE, YOU ACKNOWLEDGE YOUR ACCEPTANCE OF THE TERMS OF THIS SUBSCRIBER AGREEMENT.

D.1.1.1 By submitting a request for a NASA HSPD-12 compliant badge you agree to use the badge and any related NASA PKI certificate and services only in accordance with this Subscriber Agreement, including:

D.1.1.2 Make true representation at all times regarding information in your HSPD-12 compliant badge request, related Public Key Certificate request, and other identification and authentication information related to a NASA PKI Certificate;

D.1.1.3 Use your badge exclusively for authorized NASA business such as to gain access to NASA facilities and/or systems;

D.1.1.4 Inform NASA within 24 hours of the loss of your badge;

D.1.1.5 Take reasonable precautions to protect your badge from loss, disclosure, modification, or unauthorized use;

D.1.1.6 Inform NASA within 48 hours of a change to any information included in your HSPD- 12 compliant badge request and related Public Key Certificate application;

D.1.1.7 Return the badge to NASA upon expiration, demand by NASA, or when you no longer require the badge, for reasons including job transfer, extended leave, resignation, or termination of employment. NASA HSPD-12 compliant badge contains a NASA Public Key Certificate suitable for providing authentication.

D.1.1.8 Failure to abide by NASA certificate policies and practices may constitute grounds for revocation of certificate privileges, and may result in administrative action and/or criminal prosecution under the computer fraud and abuse act (18 U.S.C Sec. 1030 (c)). NASA reserves the right to refuse to issue a NASA Public Key Certificate. Additional information regarding NASA Public Key Certificates is available at http://nasaca.nasa.gov/docs.html.

D.1.1.9 This agreement shall be governed by and construed in accordance with United States Federal law. NASA badges and Public Key Certificates are deemed Government supplied equipment, and as such, all users are bound by U.S. Federal law governing the use of Government provided equipment.

D.1.1.10 If any provision of this Agreement is declared by a court of competent jurisdiction to be invalid, illegal, or unenforceable, all other provisions shall remain in force. Further information, including HSPD-12 badge applicant rights and responsibilities, is available on the Agency Web site at http://hspd12.nasa.gov.

D.2 Account Access:

The following statement describes your responsibility for using the badge for logical access to NASA computer assets: Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Federal law; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of assigned accounts and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording, and I will have no expectation of privacy in my use of and content on these systems and the computer equipment. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution. (NPR 2810.1A, 11.3.3.2)

D.3 Statement:

I hereby certify that the information provided by me is true and correct to the best of my knowledge and belief. I certify that I am the individual described in the NASA badge request. I agree to maintain control of the badge at all times once my fingerprint activates it and upon receipt and to abide by the agreements above. Once issued to me, I will immediately notify the Center Protective Services Office (Security) if I discover that it is not under my control due to misplacement, loss, or other cause.

This document does not bind the public, except as authorized by law or as incorporated into a contract. This document is uncontrolled when printed. Check the NASA Online Directives Information System (NODIS) Library to verify that this is the correct version before use: https://nodis3.gsfc.nasa.gov.

Appendix E: References

a. Immigration and Nationality, 8 U.S.C. § 1101.

b. Unfair Immigration-Related Employment Practices, 8 U.S.C. § 1324.

c. Violation of Regulations of National Aeronautics and Space Administration, 18 U.S.C. § 799.

d. Uniform Administrative Requirements, Cost Principles, and Audit Requirements For Federal Awards, 2 CFR 1800.913 Investigative Requirements.

e. Security Requirements for Government Employment, E.O. 10450, 3 CFR part 936, (1949-1953).

f. Equal Employment Opportunity, E.O. 11246, 3 CFR, (1964-1965 Comp).

g. Access to Classified Information, E.O. 12968, 3 CFR 391, (1995 Comp).

h. Suitability Determinations - Subpart B, 5 CFR 731.202 and 731.501.

i. Civil Service Rules, 5 CFR 7.4.

j. Federal Acquisition Regulation (FAR) Clause 52.204-9, Personal Identity Verification (PIV) of Contractor Personnel.

k. OMB Memo M-11-11, February 3, 2011, "Continued Implementation of Homeland Security Presidential Directive (HSPD)-12, Policy for a Common Identification Standard for Federal Employees and Contractors."

l. NPD 1371.1, Waivers of the Residence Abroad Requirement for Employees of NASA Contractors and Grantees.

m. NPD 1600.2, NASA Security Policy.

n. NPR 1050.1, Authority to Enter Into Space Act Agreements.

o. NPR 1371.1, Requests for Waivers of the Residence Abroad Requirements for Exchange Visitors Sponsored by NASA Contractors and Grantees.

p. NASA Grant Information Circular (GIC) 06-02, September 22, 2006.

q. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations.

r. OPM Memorandum, July 31, 2008, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12."

s. 509 Certificate Policy for the U.S. Federal Public Key Infrastructure (PKI) Common Policy Framework, v2.5 October 16, 2006.